DEBRECENI EGYETEM
INFORMATIKAI KAR

WINDOWS SZERVER 2008 ÚJDONSÁGAI ÉS HÁLÓZATI MEGOLDÁSAI

Diplomamunka

Konzulens: Dr. Krausz Tamás
Egyetemi adjunktus

Készítette: Pálóczi Árpád
Programtervező matematikus
Hallgató

Debrecen, 2009

Tartalomjegyzék

I. Bevezetés

A Windows Server 2008 a Microsoft cég terméke, mely professzionális megoldásokat kínál hálózati, alkalmazási megosztás és webszolgáltatási jellegű problémákra. A Microsoft nagy részét lefedi a szoftverpiacnak, ezért is esett az ő termékére a választásom. Tanulmányomban szeretném megmutatni, hogy milyen szolgáltatásokat kínál az új Windows szerver termék, valamint milyen megoldásokat nyújt hálózatkiépítésben felmerülő problémákra. Hallgatói pályafutásom során legtöbbet Windows környezetben dolgoztam, emiatt is érzem úgy, hogy érdemes tanulmányozni a Windows Szerver 2008-at. Célom, hogy megmutassam a termék egyszerű használata mellett azt is, hogy hatékony újdonságokkal kezeli a hálózati infrastruktúrákban felmerülő kérdéseket. A téma terjedelme miatt csak az általam választott fontosabb funkciókat mutatnám be.

A mai rohanó világban fontos, hogy egy megbízható és biztonságos hálózat gyorsan kiépüljön. Windows Szerver 2008 ezeket a szempontokat figyelembe véve könnyen kezelhető megoldásokat nyújt. Egy vállalati rendszer esetén kritikus, hogy az informatikai infrastruktúrája megfelelően legyen kiépítve, biztonságos legyen, az adatok megfelelően legyenek védve a külső támadásoktól és belső károsodásoktól, úgymint a vírusoktól vagy a hardver meghibásodásoktól. Nagy vállalati környezet esetén felmerülhet az, hogy gyorsnak, könnyen kezelhetőnek és dinamikus lennie. Ha hálózatunkra csak a megfelelően beállított és vírusmentes gépek belépését szeretnénk engedélyezni, akkor erre Windows Szerver 2008 NAP-et, azaz a Hálózati Hozzáférés Védelmet kínálja nekünk megoldásként. Ugyanis történhet úgy, hogy egy vállalati hálózathoz egy laptop csatlakozik, amit napvégén a felhasználó hazavisz. Ekkor könnyen előfordúlhat, hogy a számítógép megfertőződik, vagy a felhasználó nem megfelelően tartja karban és így biztonsági rés lehet a hálózat számára. Házirenddel kizárhatjuk az ilyen gépeket, de ekkor a felhasználó nem tud részt venni a vállalat belső hálózati életében. A NAP azt a megoldást kínálja, hogy az „egészségtelen” gépeket megvizsgálja és kijavítja, így újra egészségesek lesznek, azaz a kliens újra aktív résztvevője lesz a hálózatnak. Ezzel bevezeti azt a politikát, hogy automatikusan megjavítsunk egy hálózati csomópontot és így nem zárjuk ki véglegesen a számítógépet a hálózatból.

Ilyen és hasonló elegáns megoldásokat kínál a Windows Szerver 2008.

II. A Windows Server 2008 termékcsalád

A Windows Server 2008 termékcsaládnak 6 tagja van, melyeket a következő pontokban szeretnék ismertetni.

II.1 Windows Server 2008 Standard

A valaha megjelent legrobusztusabb Windows Server operációs rendszer, amely továbbfejlesztett beépített webes és virtualizációs szolgáltatásai révén fokozza a kiszolgálói infrastruktúra megbízhatóságát és rugalmasságát, ugyanakkor segít az időráfordítás és a költségek csökkentésében. A rendszer hatékony eszközei segítségével a kiszolgálók fokozottan ellenőrizhetők, a konfigurációs és a felügyeleti feladatok pedig egyszerűbben elláthatók. A fejlettebb biztonsági funkciók fokozzák az operációs rendszer stabilitását, ami nemcsak az adatok és a hálózat védelmét segíti elő, hanem szilárd, rendkívül megbízható alapot biztosít a vállalat működése számára.

II.2 Windows Server 2008 Enterprise

Ez a kiadás nagyvállalati felhasználásra alkalmas platformot biztosít az üzleti szempontból kritikus fontosságú alkalmazások használatához. A magas rendelkezésre állást segítik a fürtszolgáltatások és a processzorok működés közbeni telepítésének lehetősége. Az összevont identitáskezelési funkciók fokozzák a rendszer biztonságát. A virtualizációs licencjogosultságok révén az alkalmazások konszolidálhatók az infrastrukturális költségek csökkentése érdekében. A Windows Server 2008 Enterprise kiadás megfelelő alapot nyújt egy rendkívül dinamikus, méretezhető IT-infrastruktúra kiépítéséhez.

II.3 Windows Server 2008 Datacenter

Ez a kiadás nagyvállalati kategóriájú platformot biztosít az üzleti szempontból kritikus fontosságú alkalmazások használatához és a nagyarányú virtualizációhoz kisebb és nagyobb kiszolgálókon. A magas rendelkezésre állást segítik a fürtszolgáltatások és a dinamikus hardverparticionálási lehetőségek. A korlátlan virtualizációs licencjogosultságok révén az alkalmazások konszolidálhatók az infrastrukturális költségek csökkentése érdekében. A rendszer 2, de akár 64 processzorral is üzemeltethető. A Windows Server 2008 Datacenter kiadás megfelelő alapot nyújt a nagyvállalati kategóriájú virtualizációs és vertikálisan méretezett (scale-up) megoldások kiépítéséhez.

II.4 Windows Web Server 2008

A feladatorientált webkiszolgálóként használható kiadás a következő generációs Windows Server 2008 rendszer webes infrastrukturális szolgáltatásai alkotta sziklaszilárd alapokra épül. Az újratervezett IIS 7.0 kiszolgálóval, valamint az ASP.NET technológiával és a Microsoft .NET-keretrendszerrel integrált Windows Web Server 2008 rendszer segítségével bármely vállalat vagy intézmény gyorsan üzembe helyezheti webhelyeit, weblapjait, webalkalmazásait és webszolgáltatásait.

II.5 Windows Server 2008 for Itanium-Based Systems

A kiadás nagyméretű adatbázisok, üzleti célú és egyéb alkalmazások kiszolgálására optimalizált, és a magas rendelkezésre állás mellett akár 64 processzorral is üzemeltethető a nagy erőforrás-igényű és a vállalat működése szempontjából kritikus fontosságú megoldások igényeinek való megfelelés érdekében.

II.6 Windows HPC Server 2008

A nagy teljesítményű számítástechnika (HPC) következő generációját jelentő Windows HPC Server 2008 nagyvállalati kategóriájú eszközöket kínál a kiemelkedően hatékony HPC-környezetek megvalósításához. A Windows Server 2008 rendszer alapjaira épülő, 64 bites technológiával működő akár több ezer processzormagra is hatékonyan méretezhető, és a rendszer állapotának és stabilitásának proaktív megfigyelésére és karbantartására szolgáló felügyeleti konzolokat tartalmaz. A feladatütemezés terén megvalósított együttműködő-képesség és rugalmasság lehetővé teszi a Windows és a Linux rendszerű HPC-platformok integrációját, továbbá biztosítja a kötegelt és a szolgáltatásorientált alkalmazás (SOA) jellegű munkaterhelések támogatását. A fokozott hatékonyság, a méretezhető teljesítmény és az egyszerű kezelhetőség csak néhány azok a jellegzetességek közül, amelyek a Windows HPC Server 2008 rendszert a legnagyszerűbb választássá teszik a Windows-környezetek esetében.

III. Telepítés

A Windows Szerver ezen kiadásával érdemes foglalkozni, valamint megtanulni hogyan telepítsük fel a szükséges szolgáltatásokat, (mint például a szerepköröket) mielőtt éles rendszerben kezdenénk el üzemeltetni. Új telepítési opciókat érhetünk el, ilyen például a Server Core telepítés, a Windows Telepítési Szolgáltatások, meglévő Windowsra telepítés és a duális indító forgatókönyvek.

Olyan új eszközökkel találkozhatunk, mellyel nem csak egyszerűbbnek találjuk majd a telepítést, hanem mostantól több lehetőségünk lesz arra, hogy csak a nekünk szükséges dolgokat tegyük fel. Például, ha szelektívek akarunk lenni és csak a minimális szolgáltatásokkal akarjuk futtatni a szerverünket, akkor a Server Core opciót választhatjuk a telepítés közben. Ha úgy akarjuk feltenni a szerverünket, hogy nincs lekezelve a válasz fájlunk, akkor erre is van egy új lehetőség, ami egyszerűbbé teszi számunkra a dolgokat. Ebben a fejezetben le szeretném fedni az alap telepítési lehetőségeket, amik akkor lesznek elérhetőek számunkra, ha teljes verziót használunk.

Fontos megjegyezni, attól függetlenül, hogy a 2008 egy jó termék (sokfajta új tulajdonsággal és fejlesztett funkcionalitással), soha sem szabad béta vagy teszt verziót használnunk éles környezetben. Nem ajánlott és nem is rendelkezik megfelelő támogatással az ilyen verziójú termék. Más új operációs rendszerekre is igaz, hogy nem szabad azonnal felállítani éles környezetben anélkül, hogy először teszteltük volna a kompatibilitását a számunkra szükséges szoftverekkel és hardverekkel.

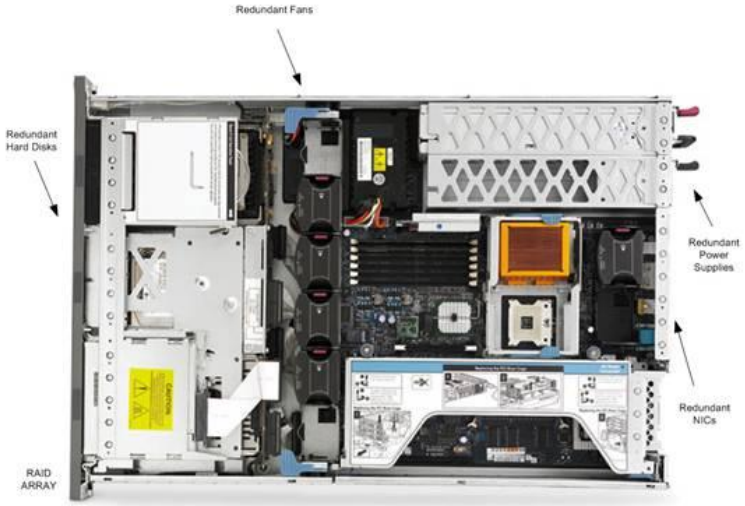
III.1 Előkészületi feladatok

Az első lépés a telepítésben, hogy elkészítünk minden olyan jellegű vizsgálatot, ami szükséges ahhoz, hogy megfelelő méretű hardvert tartalmazzon a szerver éles környezetben. Ha ezeket a lépéseket végigcsináljuk, akkor egy zökkenőmentes telepítésre számíthatunk. Az nem elég, hogy azt mondjuk felkészültünk a telepítésre. Biztosra kell menni és meg kell nézni, hogy minden szükséges szoftver rendelkezésre áll-e. Érdemes egy táblázatot készíteni arról, hogy mi szükséges, milyen lépések vannak és miket végeztünk már el. Ez elég nagy segítség lesz abban az esetben, hogy ha problémába ütköznénk, hiszen ekkor a táblázatból ki tudjuk keresni a probléma forrását, illetve utánna tudunk járni az interneten keresztül. Ajánlott egy tervet készíteni, majd letesztelni, hogy mi működik és mi nem, mielőtt feltennénk egy új rendszert a régi helyébe. Másik jó példa erre, mikor elsők között használunk egy Windows

Szerver 2008-at a még korai verziójában (Longhorn), tesztelésből kifolyólag, hamar rá ébredhettünk, hogy roppant nehéz feltepíteni egy Enterprise tipusú szerverre. Ez azért van, mert a legtöbb Enterprise szervergyártó még nem készített megfelelő drivert.

Korai példány tesztelésénél kederülhet, hogy nem kompatibilis a drivere a RAID eszközökkel, aminek köszönhetően félbeszakadhat a telepítés. A telepítési lehetőségek közül most az Enterprise szerverre való telepítést választjuk. A telepítés megtervezése bármilyen osztályú szervernél nagyon fontos lehet, ellenkező esetben problémákba ütközünk és ez időkieséssel járhat (például friss driverek megkeresése). Mikor felsőfokú felszereléssel dolgozunk elég gyakori, hogy a terjesztők support csapatával közvetlenül együtt kell dolgoznunk, hogy az újonnan kifejlesztett vezérlőprogramokat megkapjuk. Béta verziójú Windows tesztelésénél érdemes megnézni a HP, Dell és a többi hardver gyártó honlapját, hogy van-e firmware és szoftver frissítésük.

A legtöbb adatközpont a szervereiket Enterprise szintű hardveren futtatják és nem PC alapokon. Egy vállalati osztályú szerver egy olyan rendszer, amely nagy hálózatok számára lett építve és általában nagy teljesítményű, skálázható és redundáns. Amellett hogy jóval drágább, sokkal funkcionálisabb és rugalmasabb mikor telepítjük, és roppant egyszerű javítani a hibákat azok bekövetkezésekor. Ezek a szerverek képesek megszakítás nélkül futni, miközben az elromlott eszközök javításra vagy cserelésre kerülnek. Olyan vállalati osztályú programok számára lehet őket skálázni, mint az SQL szerver vagy Exchange, illetve más középkategóriás alkalmazásoknak is. Általában az ilyen fajta szerver fejlett hardvereket tartalmaz és legtöbb effajta szerver rendszer közül (Dell, HP, IBM, stb.) a saját szoftver eszközeikkel rendelkeznek. Ezek segítségével a driver és a menedzselő szofverek könnyen feltelepíthetőek Windowsra, így az tudja kezelni a vállalati szintű hardvereket. Egy példa ilyen típusú szerverre a HP DL380, ami az 1. ábrán látható.



1. ábra: Egy vállalati-osztályú szerver rendszer, HP DL380

Az 1. ábrán látható, hogy a legtöbb hadver a szerverben redundáns. Redundánsak a tápegységek, ventillátorok és hálózati csatlakozók, kettő processzor hely van, (az egyikben található is processzor) ezek miatt jobb hibatűrő képessége lesz a szervernek. A legtöbb moduláris, futás közben cserélhető, azért hogy a szerver tovább működjön olyankor is, ha hiba következne be bármelyikben. Párosítuk össze ezt még redundáns szünetmentes tápokkal és nagy valószínűséggel elérhetjük az 5 kilencest (99.999), azaz a maximális rendelkezésre állási időt. Így nem kell gyakran kikapcsolni a rendszert, legfeljebb néhány frissítés, gyors javítás és szervíz csomag futtatása esetén.

Az egyik főprobléma amellyel szembe találkozhatunk telepítés közben, a RAID telepítéséből fakad. Régebben elég nehéz volt olyan drivert találni, ami támogatatja a Windows Szerver 2008-t, manapság már meglehetősen könnyebb. Az NT 3.x és 4.0 –ban nem volt egyszerű folyamat a megfelelő meghajtó program megkeresése. Az operációs rendszer korai verzióiban (mint ahogy említésre került – NT verziók például), le kellett nyomjunk a megfelelő billentyűt (F6), hogy a RAID eszközöket hozzáadhassuk telepítés közben. Ezzel ráeröltettük a rendszerre, és ezekután még meg kellett birkóznunk vele, hogy az rendeltetésszerűen működjön, illetve stabil maradjon. Sokminden változott azóta, de egy dolog ami sosem fog az az, hogy amikor egy új rendszert piacra dobnak, a gyártóknak naprakész drivereket kell csinálni és ez bizony időt igényel. Ez sosem készül el a béta verzió alatt, így nagyon ritka az amikor teljes támogatást kapunk a teljes verzió megjelenése előttig. Szerencsénkre a Windows Szerver 2008 már jóval túl van ezen a korszakon.

Megjegyzés: Mindenképp győződjünk meg arról, hogy minden szoftver, firmware és driver amit letöltöttünk használható.

A RAID használata erősen ajánlott, illetve érdemes telepítenünk mikor egy új vállalati osztályú szervert helyezünk üzembe. A redundáns jellemzője miatt fontos lehet mikor olyan váratlan események következnek be, amelyek a szerver összeomlásához vezetnek. A RAID annyit jelent mint: Redundant Array of Inexpensive Disks, azaz Redundáns Tömb Olcsó Merevlemezekből. A 2. ábrán látható egy példa vállalati-osztályú szerverre, amelyben 6 SCSI merevlemez található. A 3. ábrán egy külső RAID tömb látható, amely összeköthető Optikával vagy SCSI-vel.

2. Ábra: Belső RAID tömb

3. Ábra: Külső RAID tömb.

RAID-nek több szintje is van, azaz többféleképpen is bekonfigurálható. A táblázatban láthatóak a legtöbbször használt RAID szintek és a hiba toleranciájuk (vagy hiányuk).

RAID szint	**Típus**	**Hibatolerancia**	**Szükséges merevlemezek**
RAID 0	Striping	Nincs	2
RAID 1	Duplexing	Van*	2
RAID 0+1	Striping + Duplexing	Van	2
RAID 5	Striping Paritással	Van	3

1. Táblázat: Általánosan használt RAID szintek

***Megjegyzés: Duplexelés és Tükrözés** hasonlóak egymáshoz, mindkettő módszer 2 lemezt használ és lemezenként tárolják az adatok egy másolatát. A fő különbség a lemez vezérlőjében van. Mikor két lemez vezérlőt használunk (lemezenként egyet), akkor ezt nevezzük duplexelésnek, ezzel növeljük a hiba toleranciát. Mikor tükrözünk, akkor csak egy vezérlő van, hiába van két lemez használatban, így maga a vezérlő válik a hiba forrásává.

Megjegyzés: A sztrippelést általában arra használják, hogy növeljék a teljesítményt olyan helyeken ahol paritást használnak, hogy rendundanciát adjanak megoldásként. Paritás köztudottan növeli a felhasznált lemez területet.
Habár több másfajta RAID szint létezik, ezek azok, amelyeket általában használni szokás manapság.

III.2 Rendszer követelmények

Mikor egy Windows Szerver 2008-at telepítünk, fontos hogy felmérjük a minimum rendszerkövetelményeket, annál a rendszernél amelyikre feltesszük. Ha a rendszer nem felel meg a minimum követelményeknek, akkor megszakad a telepítés. A 2. táblázat megmutat egy párat a szükséges és az ajánlott rendszerkövetelmények közül.

Komponens	Minimum	Ajánlott
CPU	1 GHz (x86-os esetén) vagy 1.4 GHz (for x64-es esetén)	2 GHz vagy gyorsabb
RAM	512 MB	2 GB vagy több
Merevlmez (Rendszer Partíció)	10 GB szabad terület	40 GB vagy több
Média	DVD-ROM meghajtó	DVD-ROM meghajtó
Monitor	Szuper VGA (800 x 600) vagy nagyobb felbontású monitor	Szuper VGA (800 x 600) vagy nagyobb felbontású monitor
Perifériák	Klaviatúra és egér (vagy más mutatózásra alkalmas ezköz)	Klaviatúra és egér (vagy más mutatózásra alkalmas ezköz)

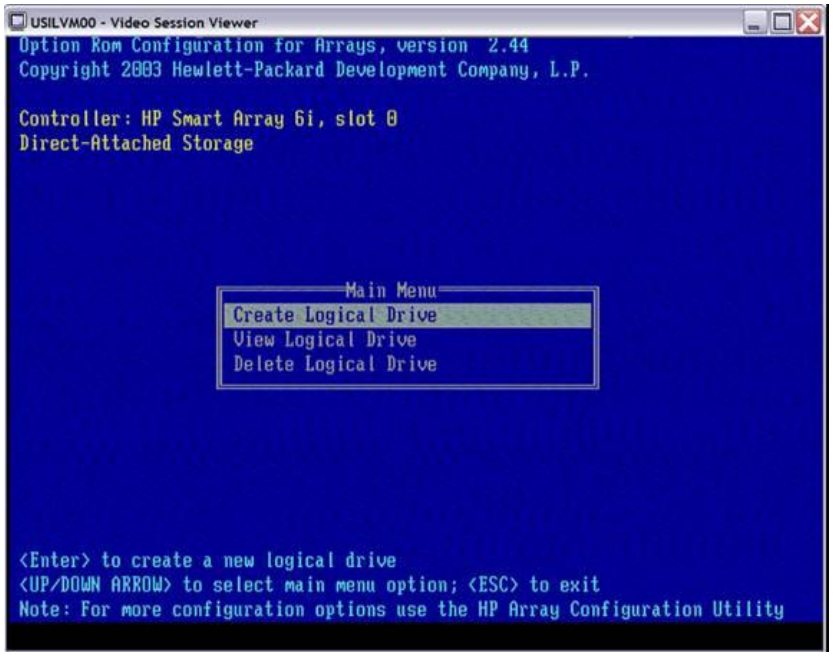
2. Táblázat: Windows Szerver 2008 rendszerkövetelmények

Mikor kalibráljuk a telepítésünket mindig jusson eszünkbe az elő-tervezés, amit már a korábbiakban tárgyaltunk. Például ha van egy adatlapunk arról, hogy a leendő szerveren milyen programok fognak futni, akkor azt időben észlelhetjük hogy bővítenünk kell például a proceszorunkat. Megtévesztőek lehetnek a kétmagos processzorok. Fel kell ismernünk, hogy a processzor teljesítménye nem csak az óra frekvenciájától, hanem a proceszorok számától és az átmeneti tár (cache) méretétől is függ. A Windows Szerver 2008 Itánium alapú rendszeréhez például egy Intel Itanium 2 processzor szükséges. Most hogy tudjuk mi kellhet, kezdjük el telepíteni a szeverünket.

III.3 Hardver beállítások

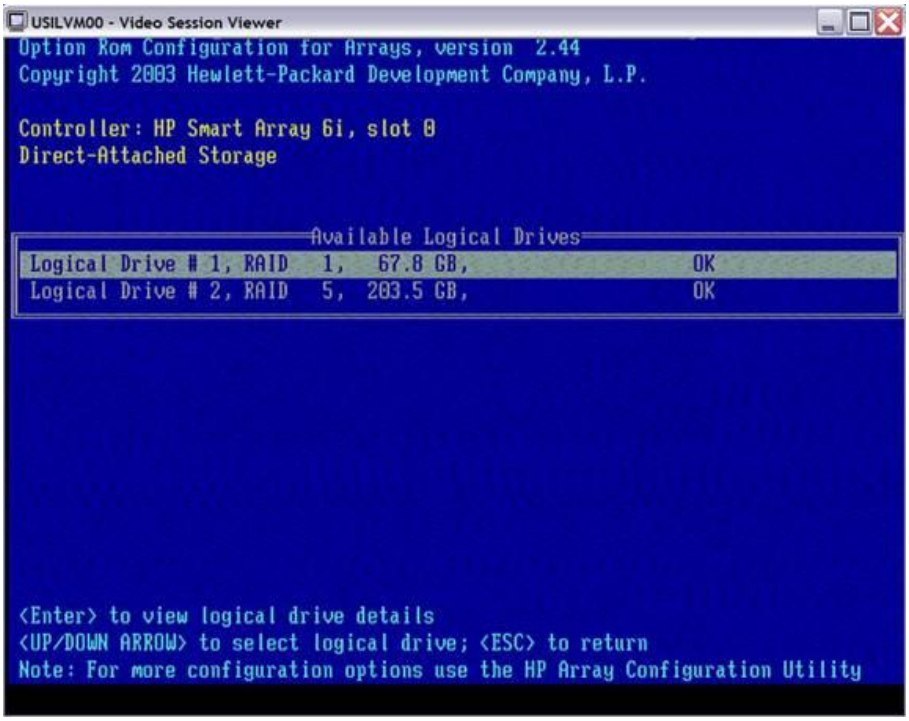
Ahhoz hogy rendesen feltelpítsünk egy Windows Szerver 2008-at, elsőnek be kell konfigurálnunk a hardvert. Mikor egy vállalati osztályú szerver rendszerrel dolgozunk, úgy mint a HP DL380, akkor be kell állítani a háttértárakat, hogy fel tudjuk telepíteni

rendszerünket a szükséges tárterületen belül. Ehhez szükségünk lehet a RAID konfigurálására. Ahhoz hogy ezt megtegyük a szerver BIOS-át kell használnunk, esetleg egy hozzátartozó konfiguráló eszközt. Példánkban a rendszer BIOS-át fogjuk használni.



4. ábra: RAID tömb beállítása

Korábbiakban már említettük, hogy többféle szintű RAID beállítás is lehet ugyanazon a szerveren. Az 4. ábra mutatja, a BIOS beállításokat a HP DL380-nál, melyen a meghajtók készen állnak a a RAID beállítására. Ebben a példában egy HP Smart Array 6i típust konfigurálunk, ami saját vezérlővel (Host Bus Adapter) rendelkezik. Az 5. ábrán látható hogyan tudjuk beállítani az eszközök redundanciáját.



5. ábra: Logikai meghajtók konfigurálása a tömben

Ha készen vannak a RAID beállításai, akkor elkezdődhet a telepítés.

Megjegyzés: Mindig használjunk RAID-et ha az lehetséges. Az előző példánkban a meghajtók már be lettek konfigurálva, így a rendszert összeomlás vagy hardver hiba esetén a RAID segítségével helyre tudjuk állítani. A lemezeket, amelyekre az operációs rendszer telepítve lett, tükrözésre állítottuk be a RAID 0+1 konfigurációban. A maradék meghajtónkat RAID 5 támogatására állítottuk be. Megelőzhetünk mindenféle katasztrófát azzal, hogy a meghajtókról készítünk egy biztonsági másolatot. A BIOS két logikai meghajtót mutat, az egyik majdnem 70 GB a másik 200 GB körüli tárterülettel rendelkezik. Mostmár fel tudjuk telepíteni Windows-unkat minden gond nélkül és lemez hiba esetén orvosolni is tudjuk azt.

III.4 Windows Szerver 2008 kézi telepítése

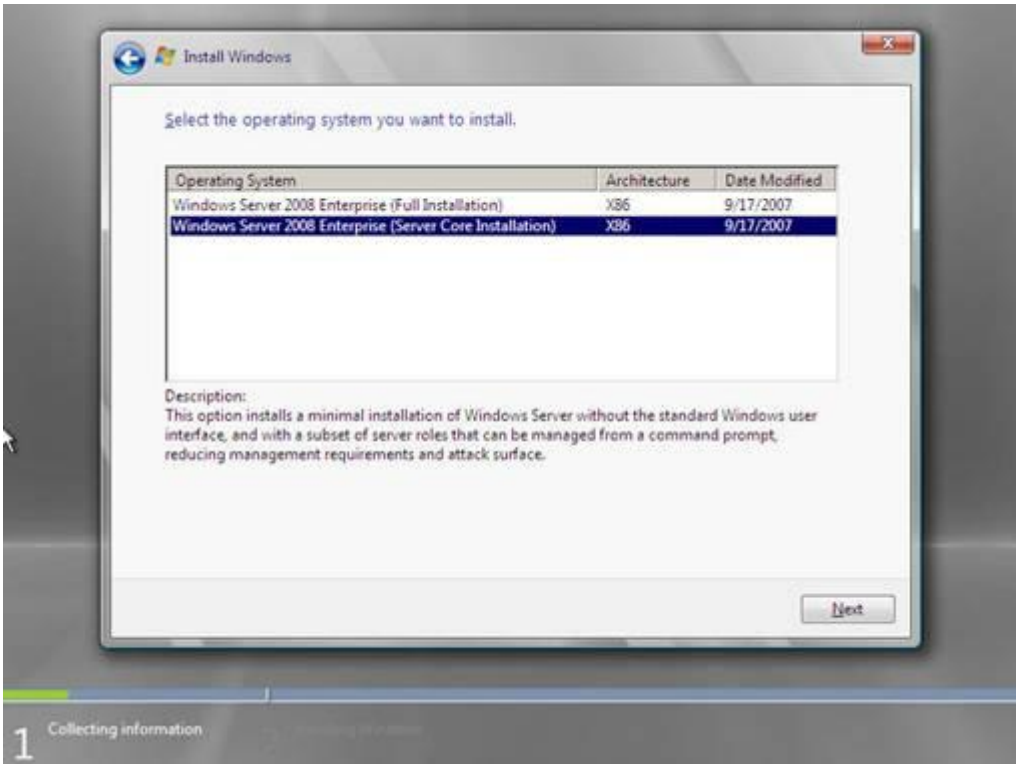
Ez az operációs rendszer kézi telepítése elég könnyűnek fog tünni. Miután meggyőződtünk arról, hogy minden előkészületet megtettünk, akár kezdhetjük is. A lista vagy munkalap amit ajánlottunk a telepítés kezdetén, nagy segítségünkre lesz azzal hogy megmutatja milyen szoftvereket készítsünk elő. Mielőtt hozzálátunk a procedurához érdemes megvizsgálni, hogy elérhető-e minden szükséges adat.

Mikor a Windows Szerver 2008-at telepítjük, láthatjuk hogy a beállítások szakaszokra vannak bontva.

1. Elsőnek is tegyük be telepítő médiát (CD/DVD-ROM-ot) és futassuk, hogy ha az automata telepítés nem indulna el. A 6. ábrán látható a kezdő dialógus. Kattintsunk a Next-re és kezdjük a telepítést. Ha egyszer kiválasztottuk az 'Install Now' –ot, akkor lehetőséget kapunk a beállítások elvégzésére és az aktivációs kulcs begépelésére.

6. ábra: Windows Szerver 2008 telepítése

2. Következőként írjuk be az aktivációs kulcsot és kattintsunk a Next-re. Ha nincs kulcsunk, akkor abszolút nem fogjuk tudni használni a szoftvert!
3. Amint begépeltük a kulcsot, kapunk egy választási lehetőséget, hogy milyen fajta telepítést szeretnénk. A 7. ábra mutatja, hogy kiválaszthatjuk a teljes telepítést (amit most ki is fogunk választani) vagy egy Server Core-t , ami csak a szükséges alapszolgáltatásokat és funkciókat telepíti fel, nem pedig a teljes redszert. A két lehetőség tehát:
   - Windows Server 2008 (Full Installation): feltelepül a teljes Windows Server 2008, ami a teljes felhasználói interfészt és az összes szerver szerepet jelenti.
   - Windows Server 2008 (Server Core Installation): Így egy minimális rendszert kapunk, amelyen az általa támogatott szerver szerepeket tudjuk futtatni parancsor interfészen keresztül.



7. ábra: Választási lehetőség: Teljes vagy Server Core telepítés

4. Következőnek fogjadjuk el a licenc feltételek és kattintsunk a Next-re a folytatáshoz. Ha nem fogadjunk el a feltételek, akkor nem tudjuk feltelepíteni a szervert.
5. Következő, elfogadhatjuk a telepítést, vagy ha a telepítő program felismer egy korábban telepített Windows-t, akkor meg fogja kérdezni, hogy alap frissítést vagy egyénit hajtson-e végre, az utóbbi egy új Windows telepítést tesz fel a rendszerünkre a régi mellé.
6. Következőként be tudjuk konfigurálni a meghajtó opciókat. Ha az 'Advanced' –et választjuk, akkor beállíthatjuk a meghajtók és partíciók specifikációit, valamint hogy hogyan akarjuk a Windowst elrendezni a meghajtókon.

Megjegyzés: Mikor a frissítés lehetőséget választjuk, meg kell bizonyosodnunk arról, hogy mit lehet és mit nem lehet átvinni a régi rendszerből az újba. Azzal hogy a Windows Server 2008-at kiadták az egyik nézet az volt, hogy Windows Server 2003-at lehessen frissíteni, ugyanis ez a legtöbb vásárló által használt rendszer. Ha Windows Server 2003-at futtatunk a szerverünkön és a 2003-as alapú ADS, DNS, DHCP stb. szolgáltatásokat használunk, akkor ez a verzió a legmegfelelőbb a frissítésre.

A Microsoft azt ajánlja hogy ha nem egy ilyen ideális rendszert futtatunk, akkor teljesen új telepítést alkalmazzunk. Ebben az esetben minden adatunkról csináljunk biztonsági mentést,

majd az új rendszerre másoljuk fel és teszteljük, hogy megfelelő állapotban van-e minden adat. Mint ahogy azt korábban is említettük, érdemes tesztelni minden szoftvert, drivert, firmwiret, alkalmazást és programot a telepítés előtt. Ha a jelenlegi rendszerünket frissítjük fel akkor könnyen kiderülhet, hogy melyik alkalmazás fog majd működni és melyik okoz majd gondot.

7. Most már települnek a fájlok a rendszerre.
8. Ha véget ért a telepítés, akkor készen állunk a rendszerbe való belépésre, mint ahogy az a 8. ábrán látható.

8. ábra: Első belépés a rendszerbe

Most, hogy teljesen készen állunk a telepítéssel és rendesen fut minden, érdemes megnézni a rendszer naplófájlokat, hogy minden megfelelően települt-e. Az is segítségünkre lehet ha megnézzük a rendszernek telsejítményét terhelés nélkül, majd a várható terheléssel. Így a későbbiekben, ha gyakran megvizsgáljuk ezt, akkor könnyen megtudhatjuk, hogy minden rendben van-e vagy észlelhetjük, ha valami hiba van a gépezetben.

Ha kész a telepítésünk és be is állítottuk a rendszert, még beleütközhetünk pár problémába. Megoldásukhoz egyszerűen írjuk fel hibakódokat és figyelmeztető üzeneteket, illetve készítünk róla screenshotot. Ezután rákereshetünk a weben, könyvekben vagy újra előidézhetjük őket teszt környezetben.

III.5 Probléma megoldások

Mikor rendszerünket telepítjük belefuthatunk olyan helyzetekbe, amelyre figyelmet kell fordítani. Mint korábban is említésre került ha nem kaptunk friss drivereket a gyártóktól, akkor nagy valószínűséggel problémába fogunk ütközni telepítéskor. Még ha azt is hisszük, hogy minden megvan ami szükséges, akkor is bekövetkezhetnek váratlan események. A következő listában felsorolásra kerül pár ilyesfajta hiba:

1. Hibás, használhatatlan vagy nem támogatott driverek, firmwarek, hardverek, szoftverek és gyártói frissítések és javítások hiánya. Nem támogatott fájlrendszerek, például: FAT.
2. Áramkimaradás, ha hálózaton keresztül történik a telepítés, akkor kapcsolat megszakadása a telepítés közben.
3. Hibás a telepítési média. Ha DVD-ROM-ot használunk, megtörténhet hogy sérült a korong. Ha túl gyorsan írtunk ki adatot a lemezre, akkor az használhatatlanná vállhat.
4. Bármiféle hibaüzenetet, amit nem tudunk azonosítani, azt meg kell nézni a Microsoft Támogatás és Tudás honlapján a felvilágosodás érdekében.

Megjegyzés: Ha a frissített telepítéssel lenne gondunk, akkor győződjönk meg arról, hogy a megfelelő telepítési utat választottuk a Microsoft ajánlása alapján:

- Windows Szerver 2003 Standard Edition (R2, SP1 vagy SP2) használói Windows Szerver 2008 Standard Edition vagy Enterprise Edition verzióit telepíthetik.
- Windows Szerver 2003 Enterprise Edition (R2, SP1 or SP2) használói Windows Szerver 2008 Enterprise Edition verzióját telepíthetik.
- Windows Szerver 2003 Datacenter Edition (R2, SP1 or SP2) használói Windows Szerver 2008 Datacenter Edition verzióját telepíthetik.

III.6 Összefoglalás

Ebben a fejezetben tárgyaltunk az alapvető lehetőségekről a vállalati szerverre való telepítésnél. Megnéztük a kezdeti felkészüléseket, telepítési lépéseket és kikötéseket tettünk, amikre figyelnünk kell majd. Megtanultuk a Windows Server 2008 egy telepítésének módját, a RAID bekonfigurálását, valamint bizonyosságot kaptunk arról, hogy mindez megfelelően történt-e.

IV. Újdonságok

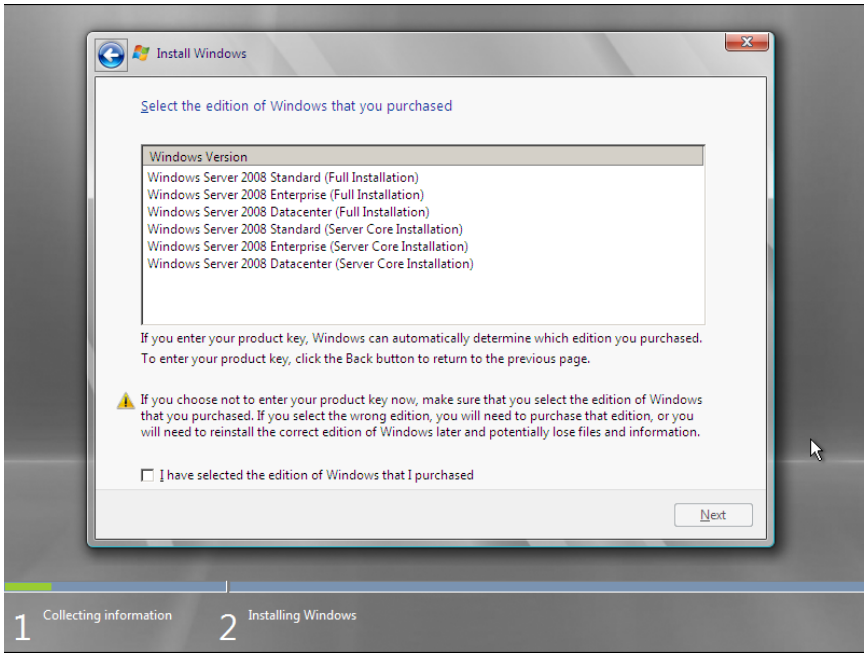
Mint az ahogy a fejezet címéből is kederül ebben a részben a Windows Server 2008 újdonságait fogom tárgyalni. Ez a Windows Server 2003-hoz képest a következőkkel bővült, melyeket a későbbiekben ismertetni is fogok: Server Core, Hyper-V, Terminal Services, Active Directory, NAP, Read Only Domain Controllers, Windows Advanced Firewall és Policy Based QoS, Secure Socket Tunneling Protocol (SSTP).

IV.1 Server Core

A "Server Core" egy olyan verziótól független telepítési mód melynek segítségével csak az operációs rendszer legalapvetőbb szolgáltatásai kerülnek telepítésre, ezzel garantálva a könnyebb menedzselhetőséget és a kisebb támadási felületet.

A kiszolgálók esetén általánosnak mondható, hogy csak egy vagy kevés feladatkört kell ellátniuk, ezért az ilyen esetekben a legtöbb szolgáltatás feleslegesen kerül telepítésre, ezzel növelve a biztonsági kockázatot, bonyolítva a menedzselhetőséget, a karbantartást és a hibaelhárítást. Vegyünk például egy Windows Server 2003-at, ahol egy DHCP szerver üzemeltetéséhez telepítenünk kell sok olyan szolgáltatást, amelyekre egyáltalán nincsen szükségünk, ilyen például az Internet Explorer, a shell, vagy egyéb háttérben futó szolgáltatás. Ebből kifolyólag a Windows Server 2008 telepítőjében találkozhatunk egy új lehetőséggel, a már említett Core opcióval, melynek segítségével csak a szükséges dolgok kerülnek a számítógépünkre. Ez több szempontból is előnyös: Kisebb biztonsági kockázat, erőforrásigény, lemezterület igény, valamint könnyebb menedzselhetőség, hibaelhárítás és nagyobb megbízhatóság.

A minimalizált telepítés elérhető minden normál változatból, X86 és X64 architektúra esetén is. Természetesen nem kell külön megvásárolnunk a Core verziót, csak el kell döntenünk hogy a teljes vagy a minimalizált változat kerüljön-e számítógépünkre. Telepítéskor figyelembe kell vennünk, hogy csak tiszta telepítés lehetséges, előző telepítés frissítése semmilyen formában nem érhető el.



9. ábra Telepítési lehetőségek

A fejlesztés során az operációs rendszer megszokott komponenseinek egy részét eltávolították és csak a legfontosabbak maradtak a rendszerben.

Amit biztosan nem találunk meg ebben a változatban: Grafikus felület, .NET Framework, CLR, MMC, Vezérlőpult, Internet Explorer, Windows Mail, grafikus help

Amit biztosan megtalálunk: Kernel, HAL, Eszközmeghajtók (legalábbis egy részük), szokásos alrendszerek, Winlogon, Jegyzettömb, Regedit.

A dologhoz hozzátartozik, hogy nem minden funkció érhető el ebben az esetben, de a lényegi szerepköröket telepíthetjük és használhatjuk. A következő szerepkörök és szolgáltatások használatára van lehetőség:

Active Directory Domain Services, Active Directory Lightweight Directory Services (AD LDS), Dynamic Host Configuration Protocol (DHCP) Server, DNS Server, File Services, Print Server, Streaming Media Services, Web Server (IIS).

Szolgáltatások:

Microsoft Failover Cluster, Network Load Balancing, Subsystem for UNIX-based Applications, Windows Backup, Multipath I/O, Removable Storage Management, Windows Bitlocker Drive Encryption, Simple Network Management Protocol (SNMP), Windows Internet Naming Service (WINS), Telnet client, Quality of Service (QoS).

A legészlelhetőbb változás természetesen a grafikus felület hiánya és talán a kevés tárhelyfoglalás. Érdemes tudni, hogy egy telepített core verzió körülbelül 1,3 GB helyet foglal, ellenben a teljes telepítés körülbelül 6-7 GB-ot. Ennek a minimalizációnak a

legnagyobb hatása talán az üzemeltetésben mutatkozik meg, hiszen a megszokott eszközeinkkel nem konfigurálhatjuk felügyelhetjük a rendszerünket, legalábbis lokálisan nem. Az első bejelentkezés után csupán egy konzolablakot látunk magunk előtt, továbbá a Ctrl+Alt+Del kombinációval elindíthatjuk a feladatkezelőt is. Az első beállításokat általában itt kell megtennünk néhány jól ismert régi parancs segítségével, ha nem a felügyelet nélküli telepítés mellett döntöttünk. Itt jegyezném meg hogy nem új speciális parancsokról van szó, összesen négy új utasítást tartalmaz a core verzió.

Egy pár példa a parancssori konfigurációra:

Az IP cím beállítása:

netsh interface ipv4 set address name="2" source=static address=10.1.1.40 mask=255.255.255.0 gateway=10.1.1.10

A számítógépnév beállítása:

netdom renamecomputer %computername% /newname:<név>

Szolgáltatások telepítése és eltávolítása:

ocsetup <szolgáltatás neve>

ocsetup <szolgáltatás neve> /uninstall

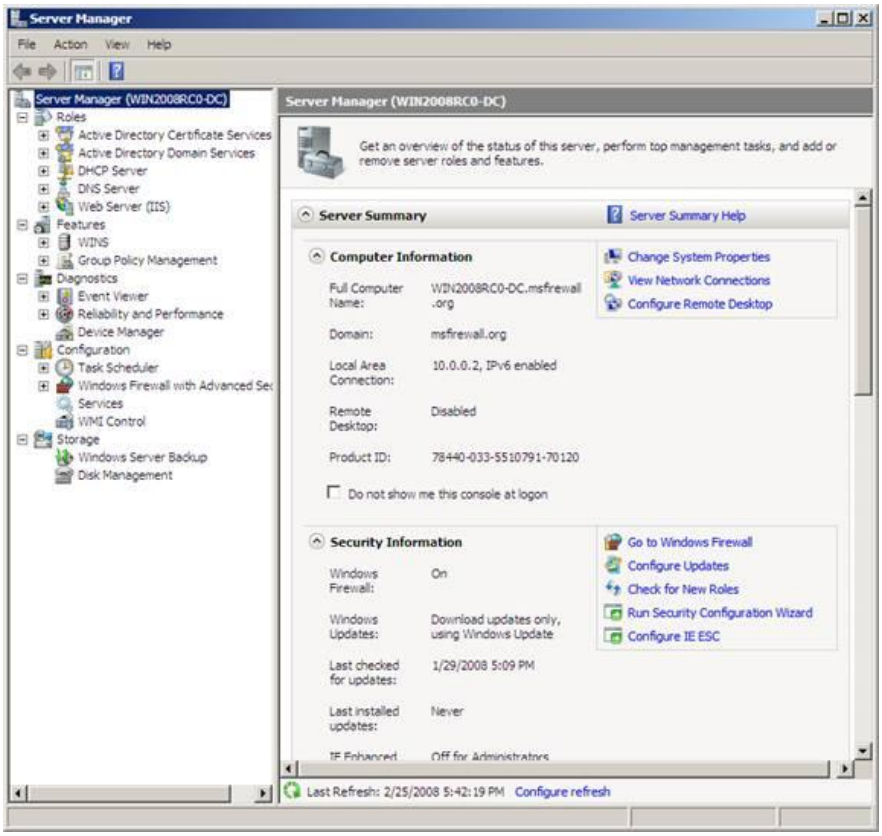
Tartományvezérlő telepítése:

dcpromo /unattend:<a szöveges válaszfájl elérési útja és neve>

Ha az első lépeseket sikeresen megtettük például dátum, számítógépnév, IP cím beállítását, ezek után már távolról is végezhetjük a további műveleteket. Ehhez használhatjuk a távoli asztalt, a winrm-et, és a szerepkörök telepítése után a szokásos MMC paneleket. Jelenleg csak Windows Server 2008 alatt érhető el az RSAT csomag, amely az adminpack utódja lesz, azonban a Vista SP1 alól is már menedzselhetjük és nem csak a Core szerverünket, hanem ezenkívűl a teljes funkcionalitású szervert is.

IV.2 Szerver menedzser és a Haladó Esemény Figyelő

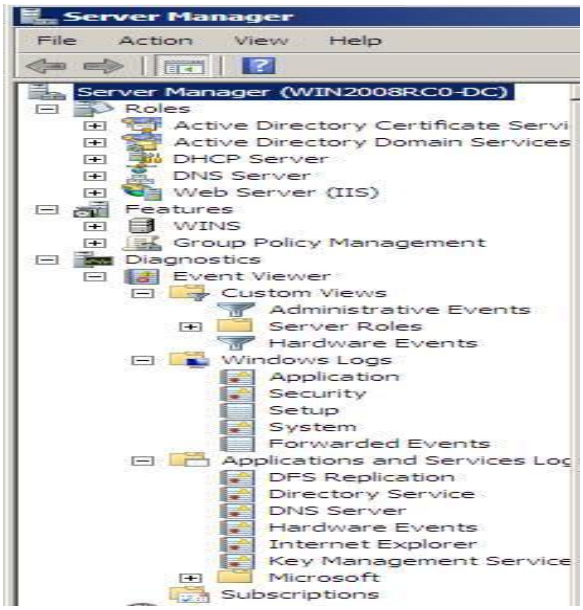
Windows Szerver 2008 tartlalmaz egy teljesen új menedzsment interfészt, amit úgy is hívhatunk, hogy Szerver Menedzser. Ezzel konfigurálni, menedzselni és felügyelni tudjuk a szerverünket. Nem olyan mint az eddigi Szerver Menedzserek amikkel találkoztunk, ez ténylegesen működik is és ezt fogjuk használni mindennap, hogy menedzseljük Windows Szerver 2008 gépünket.



10. ábra A szerver menedzser

A Szerver Menedzserben telepíthetünk szerver szerepköröket (olyanokat mint a DNS, DHCP, Activer Directory) vagy szerepkör szolgáltatásokat (pl.: Terminal Services Gateway és RRAS). Mikor a Szerver Szerepköröket és a Szerepkör szolgáltatásokat feltelepítettük, az MMC konzolok ezen szolgáltatások számára automatikusan feltelepülnek a Szerver Menedzserben. Mostantól nem szükséges létrehoznunk a saját egyéni MMC-nket.

A Szerver Menedzser ezenkívül felfedi az új és Haladó Esemény Figyelőjét. Ez nem a régi fajta eseményfigyelő rendszer, biztonság és alkalmazás csomópontokkal. Windows Server 2008 esemény figyelője eseménynaplókat nyújt számunkra. Vannak a szokásos Windows Esemény Naplók: alkalmazások, biztonság és rendszer, ezenkívűl mostantól képesek leszünk rá, hogy lássuk az eseményeket az összes olyan alkalmazásról és szolgáltatásról, amelyek fel lettek telepítve a számítógépünkre. Még hozzájön ehhez, hogy létrehozhatjuk a saját egyéni nézeteinket az Esemény Naplóban, azaz megcsinálhatjuk a saját konténereinket az események számára, az általunk választott szűrők alapján.



11. ábra Az esemény figyelő és benne pár kategória

Az egyik újdonsága az Esemény Naplónak, hogy képesek leszünk feliratkozni Eseményekre, melyek másik számítógépen futnak a hálózatunkon. Ez lehetőséget ad arra, hogy összegyűjtsünk más számítógépen található Esemény Napló adatokat a szűrőink alapján, melyeket mi konfigurálhatunk. Ily módon be tudjuk állítani a szűrőket a kritikus eseményekre, a legfontosabb szerverek számára a hálózatunkon.

Egy másik izgalmas újdonság, a beépített MMC 3.0 modul, amely lehetőséget ad rá, hogy erről a felületről végezzük el mindennapos feladatainkat is. Konkrét példaként említeném a jól ismert "Active Directory Users & Computers" modult, az adminisztrátorok által talán leggyakrabban és legtöbbet használt eszközt. Amennyiben az Active Directory telepítve van, ez minden gond nélkül elérhető a Server Manager felületéről, valamint nem új ablakban, hanem közvetlenül a manager középső oszlopában. Ha szolgáltatásokat próbálunk aktiválni a szokásos "Add/remove programs/Windows components" vezérlőpult-modulon keresztül, észrevehetjük, hogy ebben az esetben is a Szerver Menedzser segítségünkre lesz.

Kizárólag a feltétlenül szükséges összetevők telepítése történik meg és csak a szolgáltatás helyes és biztonságos működéséhez elengedhetetlen portok kerülnek megnyitásra a tűzfalon. Ennek ellenőrzéséhez és beállításához eddig a Security Configuration Wizard (SCW) eszközre volt szükség amely most is elérhető, viszont alapesetben már nem szükséges a használata. Természetesen egyéb szervertermékek, mint például SQL Server, Exchange Server esetében továbbra is érdemes használni.

Fontos megjegyeznem, hogy a Server Manager grafikus formájában csak a helyi számítógép kezelésére alkalmas, nincsen lehetőségünk távoli számítógépekhez csatlakozni az eszköz

használatával. Amiért külön kiemeltem a grafikus felület szót annak az az oka, hogy létezik egy parancssoros verzió is, mely úgyszintén alkalmatlan távoli számítógépek felügyeletére, viszont nincsen akadálya a WinRM-el (távoli számítógépkezelési protokoll) kombinált használatnak. A Server Manager parancssoros változatának indítása nagyon egyszerű, a *servermanagercmd* paranccsal indítható.

A Core változat alatt nem érhető el a Server Manager. Amiért viszont nagyon hasznos ez a parancs, az az automatizálás és a távoli menedzsment. Paraméterek segítségével lekérdezhetjük a jelenleg a rendszerben található szerepkörök listáját, és szükség szerint hozzáadhatunk újakat vagy eltávolíthatunk belőlük.

Akár XML formátumú fájlt is használhatunk mind a konfigurációs adatok exportálása, mind azok automatizálása során. Ennek különösen akkor vesszük hasznát, ha egy már meglévő szerveren található szerepköröket szeretnénk több más kiszolgálóra is telepíteni. Ilyenkor nincs más teendőnk, mint exportálni a beállításokat egy XML fájlba a következő módon: *servermanagercmd -query result.xml*

A másik szerveren pedig a következő utasítás kiadásával telepíthetjük az összetevőket: *servermanagercmd -inputpath install.xml*

A parancs egyik érdekessége a "*-whatif*" kapcsoló, amellyel a változtatások alkalmazása nélkül tekinthetjük meg mi történne, ha telepítenénk vagy eltávolítanánk összetevőket. Megtudhatjuk, pontosan milyen szolgáltatások járnak együtt a kívánt szerepkörrel, illetve hogy szükség lesz-e például a gép újraindítására.

Eddigiekben jórészt a helyi gépen történő beállításokról esett szó, most nézzük mit tehetünk meg távolról. Természetesen a távoli asztalt (RDP) bármikor használhatjuk, azonban a régi verziókból ismerős lehet egy másik nagyon hasznos csomag is, a Windows Server 2003 Administration Tools Pack, röviden "Adminpak". Ez a csomag MMC modulokat tartalmazott melyek segítségével egy távoli Windows Server, vagy akár XP alól is elérhettük a szerver szolgáltatásainak kezelőfelületét. Az eszköz most is létezik, de a Remote Server Administration Tools (RSAT) nevet kapta. Az adminpak-kal ellentétben már lehetőségünk van kiválasztani milyen eszközöket szeretnénk telepíteni, amire alapesetben az elődje nem adott lehetőséget, bár a KB314978 számú tudásbáziscikk útmutatásai alapján megoldható volt a dolog. Jelenleg az RSAT csak Windows Server 2008 alatt érhető el és a szolgáltatások közül telepíthető. Szolgáltatások, amik kezelésére lehetőségünk van:

Szerepkörök: Active Directory Domain Services, Active Directory Certificate Services, Active Directory Lightweight Directory Services, Active Directory Rights Management

Services, DNS Server, Fax Server, File Server, Network Policy and Access Services, Print Services, Terminal Services, Web Server (IIS), Windows Deployment Services
Funkciók: BitLocker Drive Encryption, BITS Server Extensions, Failover Clustering, Network Load Balancing, Simple SAN Management, SMTP Server, Windows System Resource Management (WSRM), WINS Server.
Természetesen az említett lehetőségeken kívül más módokon is felügyelhetjük kiszolgálóinkat. Ezekről most csak felsorolásszerűen: Group Policy (csoporházirend), WMI (Windows Management Instumentation felület), PowerShell, Microsoft System Center.
Nincs olyan kiforrott mint a System Center Operations Manager, azonban nagyon jó megoldás azon vállalatok számára amelyek nem akarnak pénzt kiadni a SCOM-ra.

IV.3 NAP (Network Access Protection)

A vállalatok életében eljön az a pillanat mikor a nagy kiterjedésű és több szintű hálózatok biztonságossá tétele már nehézkessé válik. Főképp nem a hálózati forgalom szabályozása és a titkosítás lesz a probléma, hanem olyan kritikus dolgok elhárítása és megelőzése, amit például egy hálózathoz kapcsolódó számítógép jelenthet az egész infrastruktúrára nézve. Egy nagy vállalathoz jellemzően rengeteg munkaállomás kapcsolódik, melyek lehetnek irodákba telepített számítógépek, laptopok, kéziszámítógépek. Ezeket az alkalmazottak otthon és a vállalaton belül, valamint nyilvános helyen egyaránt használják. Rohamosan terjednek el a cégeknél a távmunka megoldások, így az alkalmazott otthoni környezetből csatlakozik a vállalati hálózathoz, VPN-en (Virtual Private Network) vagy egyéb távkapcsolaton keresztül.
A védelem érdekében megtehetünk jópár biztonsági lépést, korlátozhatjuk a hálózatra kapcsolódó számítógépek fizikai (MAC) címeit statikus DCHP szolgáltatás alkalmazásával, ISA szerver segítsével szűrni lehet a hálózati forgalmat, házirend segítségével telepíthetünk vírusírtókat, korlátozhatjuk a hálózati portokat. Így viszont egyetlen nagy probléma vetődik fel, mi van olyankor ha egy számítógép mely számára már engedélyeztük a hozzáférést, később veszélyforrássá válik.
Feltételezzük, hogy egy hordozható számítógépet használó alkalmazott tartományi tag és mikor visszatér a munkába egy vírust hoz magával. Természetesen lehetőség van arra, hogy telepítünk a hálózati kliensekre víruskeresőket, de ezt az alkalmazott véletlenül vagy tudatosan kiiktathatja. Vannak frissítések is, ezeket sem tudjuk ellenőrizni, hogy minden feltétlenül fontos javítás fel lett-e telepítve a számítógépre. Valójában sok problémát megoldhatunk a házirendek segítségével, de ez nem ad teljesen kielégítő megoldást, így nem

biztosít elég nagy védelmet számunkra, valamint nem feltétlenül szeretnénk, hogy minden hálózatunkba kerülő számítógépre csoportházirend kerüljön. A fizikai cím korlátozása a DHCP-vel nem a dinamikus megoldások közé tartozik, így újabb feladatok merülhetnek fel. Ilyen helyzetekre nyújt megoldást a Network Acces Protection (NAP) szolgáltatás, amely segítsével a kliensek hozzáférését tudjuk szabályozni.

A Hálózati Elérés Védelem (HEV), angol nevén Network Access Protection (NAP), lehetőséget ad nekünk, hogy irányítsuk a hozzáférését minden olyan számítógépnek amelyek a hálózatunkhoz kapcsolódik. A Microsoft szerint a NAP nem pont egy biztonsági módszertan, hanem inkább egy „kliens egészség" mechanizmus, aminek segítségével lehetőséget kapunk, hogy létrehozzunk olyan házirendeket melyek meghatároznak egy minimum kliens egészségi állapotot, mielőtt a számítógép csatlakozhatna másik számítógépekhez a hálózaton. Mi is az "egészséges" állapot? Egészségesnek nevezzük azt az állapotot, amikor a számítógépek megfelelnek azon feltételeknek amelyeket a NAP házirendben meghatároztunk. Eltérő környezetekben tehát előfordulhat, hogy az egyik hálózatban egészségesnek mondott gép, nem lesz egészséges egy idegen hálózatban.

Ha röviden akarjuk megmagyarázni mi is a NAP, talán a következő meghatározás áll a legközelebb a valósághoz: a NAP biztosítja, hogy csak egészséges kliensek férhessenek hozzá a hálózati erőforrásokhoz és nem csak ennek megállapítását teszi lehetővé, de segít is elérni ezt az egészséges (elégséges) állapotot. A kliensek lehetnek asztali számítógépek, laptopok, PDA-k, és egyéb más eszközök is, melyek támogatják a NAP -ot.

NAP a Windows Server infrastruktúrától függ. Szükségünk lesz egy hálózati házirend szerverre, hogy tároljuk az egészség házirendünket. Van egy pár fajta módszer, hogy vezéreljük a hozzáférést a hálózathoz: IPSec, DCHP, 801.x és VPN megkötések. Amely gépek nem rendelkeznek a biztonság beállítási követelményekkel, azoknak nem engedélyezett semmilyen módszer használata az előzőek közül. Azonban a NAP megengedi, hogy létrehozzunk egy karantén hálózatot amire az egészségtelen kliensek kapcslódhatnak, hogy meggyógyítsák magukat. Ha egyszer a NAP kliens észleli, hogy a gép végzett a gyógyulással, akkor üzenetet küld a NAP szerver oldali komponensnek, ami válasz üzenetben elküldi, hogy rendben van csatlakozhat a hálózatra. A NAP egy nagyon jó megoldás a hálózati hozzáférés vezérlésére és ez az amire vártunk már 2003 – 2004 óta. Jó időbe tellett míg megérkezett, de érdemes volt várni rá. Sok hálózati adminisztrátor gondolja úgy, hogy a NAP az elsődleges ok arra, hogy feltelepítsük a Windows Server 2008-at, nehezen tudnánk velük nem egyet érteni.

A főként felmerülő problémák a kövezkezők lehetnek:

- Nagyon sok olyan kliens kapcsolódik más és más fizikai helyekről, amelyeket nem tudunk leellenőrizni.
- Nem tudjuk megnézni, hogy a tűzfalnak, vírusírtónak és a frissítéseknek milyen az állapota.
- A hálózathoz csatlakozó számítógépeken lehetséges, hogy nem Windows operációs rendszerek futnak.
- A csoport házirend nem ad megfelelő biztonsági szintet, mivel csak egy lehetőség a korlátozásra.

A NAP álltal nyújtott megoldás nem teljesen új keletű, mivel hasonló már az előző szerver verzióban is létezett. Ez volt a NAQC (Network Access Quarantine Control), ellenben a NAQC –kat csak távolról kapcsolódó számítógépek felügyeletére használhattuk. Másik nagy hátránya, hogy egy-egy szabály megírása önmagában is nehézkes és időigényes, ehhez még hozzájön, hogy környezetenként különböző szabályokat kell megírnunk.

Egy másik megoldás a Cisco műhelyéből került elő, amit NAC (Network Admission Control) –nak neveznek. Ez már jóval közelebb áll a Microsoft NAP-jához. Ami fontos lehet, hogy a két technológia képes arra, hogy közösen működjenek, így párhuzamosan kezelhetjük a hálózatunkat mindkét szolgáltatással egyszerre.

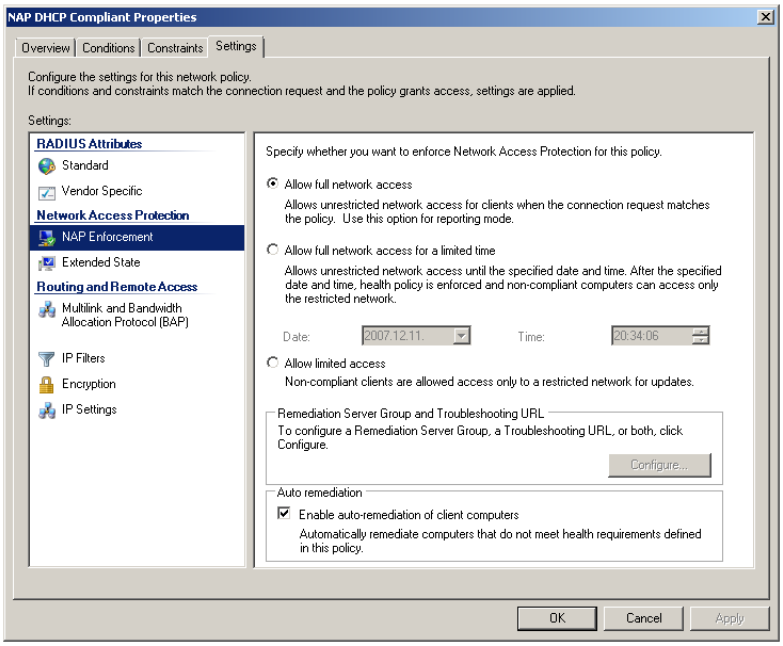
Ezenkívűl a NAP nem csak egy szolgáltatás, hanem egy platform, mely két részből áll szerver és kliens komponensből. Linux operációs rendszerekhez is létezik NAP kliens, tehát a Microsoft nem zárkózott be a saját szoftvereivel telepített hálózatba, hanem utatt nyitott más operációs rendszerek számára is.

13. ábra NAP Health Agent

A NAP segítségével megvizsgálhatjuk a kliensek állapotát, és elérhetjük, hogy a megfelelő állapotba kerüljenek. Ezenkívűl meghatározhatjuk, hogy milyen kliensek férjenek hozzá a hálózathoz, valamint monitorozhatjuk hálózatunkat.
Íme az öt módszer amelyet a NAP biztosít, és melyek segítségével szabályozhatjuk a hálózati hozzáférést.

IV.3.1 DHCP

Ennél a módszernél nem sok problémánk akad a beállításoknál, azonban ez a legvédtelenebb. A DHCP szolgáltatás segítségével korlátozhatjuk a számítógépek hozzáférését a hálózathoz. Emellett szükséges lesz egy NPS (Network Policy Server), valamint egy DHCP szerver, amelyek akár ugyanazon számítógépen is futhatnak. A munkamenet: Elsőnek a kliens kapcsolódik a DHCP szervervez IP címért valamint, hogy csatlakozhasson a hálózathoz.
A NAP megnézi a kliens állapotát, ha az egészséges ad neki egy érvényes IP címet. Különben a kliens egy korlátozott hálózati hozzáférést kap, így egy alhálózati maszkot és host route-ot kap a NAP-től, hogy eljuthasson a remediation (gyógyító) szerverhez.
A gyógyító szerverek segítséget nyújtanak a kliens javításához, (pl víruskereső frissítést), hogy a kliens egészséges állapotba kerüljön. Ilyen szerverek: WSUS (Windows Server Update Services) vagy SCCM (System Center Configuration Manager) 2007
Ha sikerült a klienst megfelelő állapotba hozni akkor kap egy olyan IP-címet mellyel már csatlakozhat az egész hálózathoz.



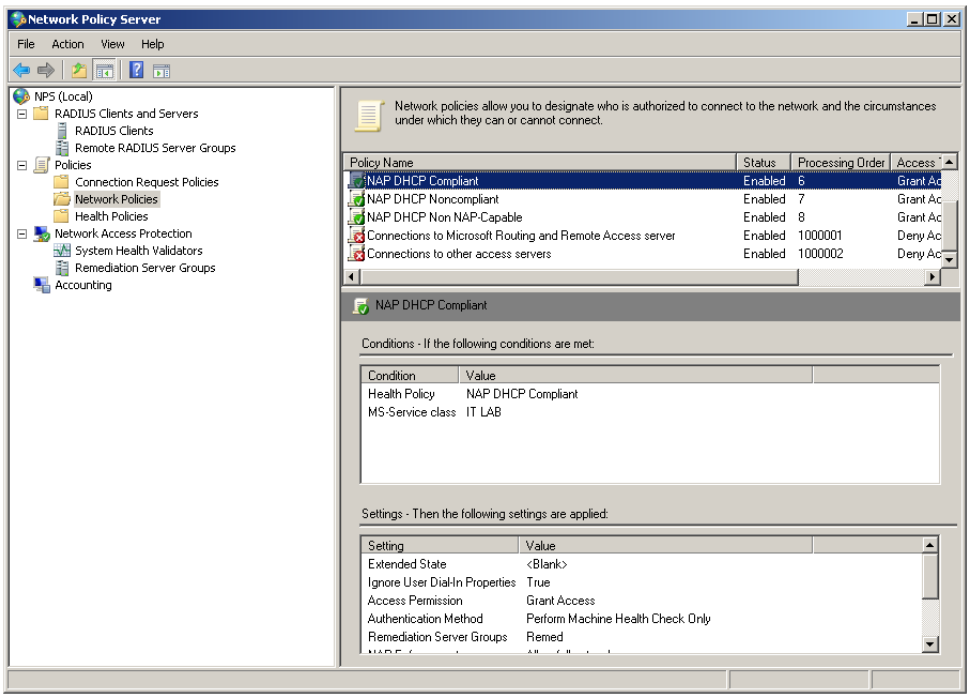
14. ábra NAP DHCP Enforcer

IV.3.2 VPN

A VPN és RRAS(Routing and Remote Access) szolgáltatásnak telepítve kell hogy legyen a Windows Server 2008 operációs rendszeren, hogy alkalmazni tudjuk ezt a metódust.

A kliens kapcsolódik a VPN szerverhez, majd a VPN szerver leteszteli a kliens állapotát a NAP használatával. Ha a kliens megfelelő állapotban van akkor kapcsolódhat a hálózathoz. Ellenkező esetben csomagszűrők kerülnek alkalmazásra és a kliens csak a korlátozott hálózathoz férhet hozzá, melyben a gyógyító szerver található.

Ha a kliens meggyógyúl a szűrők megszűnnek és a kliens hozzáférést kap a teljes hálózathoz.



15. ábra NAP hálózati beállítások

IV.3.3 802.1X

Az IEEE szabvány 802.1X protokolja hálózati elérés port korlátozását biztosítja. Azaz a fizikai hálózat alapján fogunk szabályozni. Ha egy switch-hez kapcsolódó csomópont számára engedélyezett a forgalom, akkor a port nyitott, különben tiltott.

- Egy EAP-képes számítógép kapcsolódik egy 802.1X-et támogató switch-hez. A 802.1X és a V-LAN switching támogatás szükséges a NAP megfelelő üzemeléséhez.
- Ezután a switch továbbküldi az információkat az NPS-hez, ami leteszteli a kapcsolódó kliens állapotát. Ha az pozitív, az NPS üzenetet küld a switchnek a port megnyitására,

különben portzárás történik, vagy a kliens egy VLAN szegmensbe kerül amelyben van egy gyógyító szerver.

- Az egészséges állapotba való kerülés után a port megnyílik és hozzáférhet a teljes hálózathoz.

IV.3.4 IPSec

A metódus azt a megoldást választja, hogy ha nem egészséges a kliens akkor az nem kap tanúsítványt tőle, azaz a többi kliens nem fogadja el tőle a nem megfelelő állapotú csomagokat. Az eddigi megoldásokkal ellentétben tehát itt nem jön létre egy korlátozott hálózat.

IV.3.5 TS Gateway

Ezen módszerről részletesen a következő fejezetekben tárgyalunk majd, most nézzük meg a NAP-pel való kapcsolatát. Lehetőségünk van arra, hogy a NAP-vel együtt használjuk, ám itt is csak a kizárást valósíthatjuk meg, nem tudunk automatikus gyógyító mechanizmust felépíteni. A hálózati diagnosztika eszköz segítségével gyorsan és könnyen tudunk információt kérdezni a hálózati infrastruktúráról. Az eszköz információt ad az operációs rendszerről, a számítógépről, a hálózati adapterekről és magáról a hálózatról is.

IV.3.6 Tanácsok a NAP bevezetéséhez

A hirtelen változások esetén krízisek következhetnek be, ezért erőteljesen javallott, hogy a NAP-et fokozatosan vezessük be a meglévő rendszerünkbe. Ez azért fontos, mert a hálózatban lévő csomópontok állapota nem feltétlenül megfelelő szintű a NAP bevezetésének pillanatában. Így akár az is megeshet, hogy mindent megfelelően bekonfigurálunk az egyik nap és másnap az egész hálózat áll, mert a kliensek le vannak tiltva és gyógyító szervernél állnak sorban.

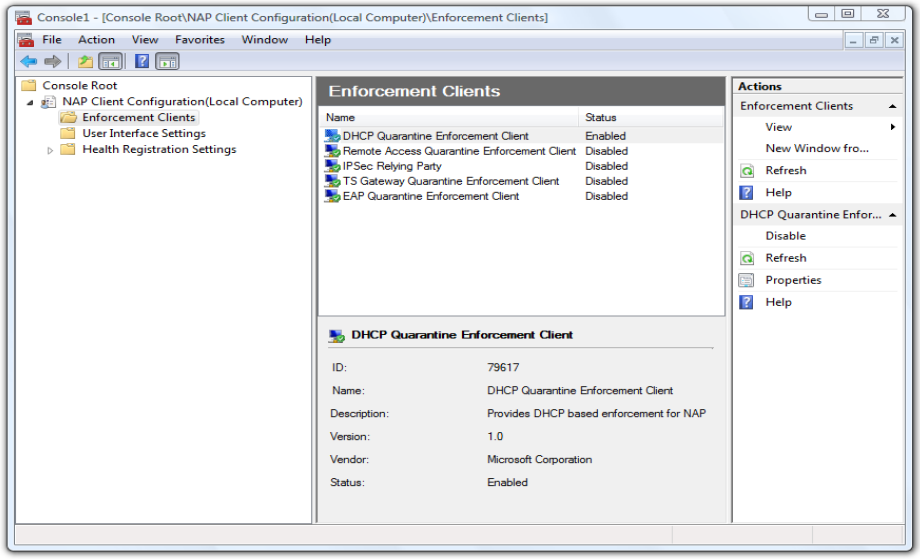
A lépések tehát a következők lehetnek:

- Elsőnek érdemes mindössze jelentéseket készíteni az eseménynaplóba, a kliensek elérés korlátozása és állapotának változtatása nélkül. Ezzel információt kaphatunk a hálózatunk jelenlegi állapotáról.
- Másodjára még mindig nem kezdjük meg a kizárást, viszont a gyógyító szervereket beiktatjuk és megkezdjük a rossz állapotú kliensek javítását.

- Harmadjára már kizárhatjuk a hálózatról azokat a klienseket, amelyeket még nincsenek megfelelő állapotban és gyógyításra szorulnak. Viszont mindezt csak egy bizonyos idő elteltével érdemese megtenni. Tehát a kizárás csak időkorlát alapon menjen.
- Végül mostmár beimplementálhatjuk a NAP-et teljes valójában, azaz ha egy kliens nem megfelelő állapotú, akkor az azonnal a karantén hálózatba kerül. Ott egy gyógyító szerver segítségével, ha már megfelelő állapotba került újra hozzáférhet a teljes hálózathoz.

IV.3.7 NAP kliens

A NAP szolgáltatást minden olyan számítógép igénybe veheti, amely képes futtatni a NAP klienst. Beépítve a Windows Vista Service Pack 1-ben és a Windows Server 2008-ban találhatjuk meg, valamint le tudjuk tölteni a Windows Server 2003-hoz és a Windows XP Service Pack 2-es operációs rendszerekhez is. Ezenkívül béta változat elérhető a Linux operációs rendszerekhez is. Természetesen a jövőben bővülni fog a NAP kliens elérhetősége. A konfigurálást a házirend segítségével érdemes végrehajtani, a számítógépen a következő parancsot kell kiadnunk: napclcfg.msc



16. ábra A Vista NAP-kliense

IV.3.8 Összefoglalás

A fejezetben láthattuk milyen újszerű biztonsági megoldásokat ad a NAP módszereivel, valamint kompatibilitásának tárházát is olvashattuk. Így elmondhatjuk, hogy a Microsoft már

nem zárkózik el a saját termékei hálózatában, hanem nyitottá vált a más gyártók operációs rendszerei felé is.

IV.4 Terminálszolgáltatások

A Windows NT 4 óta ismert a terminálszolgáltatás Microsoft szerver oldali operációs rendszereiben, de akkor még csak a saját verzióban volt elhelyezve a szolgáltatás, mely Windows NT4 Terminal Server Edition néven futott.

A már ismerős Távoli asztal kapcsolat vagy angol nevén Remote Desktop Connection, a kliens operációs rendszerekben is fellelhető. Használatával igénybe vehetjük a Terminál Server szolgáltatásait, azaz más számítógépekre kapcsolódhatunk bizonyos feladatok elvégzése végett. Telepítése után az úgynevezett távfelügyeleti (Remote Administration) mód az alapbeállítás, amellyel párhuzamosan három kapcsolódást engedélyez, 1 helyit és 2 távolit. Ez a korlát 1+1-re változott, valamint ezzel együtt a konfiguráció is, ugyanis mostantól Terminál Szerver módban annyi kliens csatlakozhat, amennyi licencet megvásárolunk. Olyan helyzetben szoktunk élni ezzel a szolgáltatással, ahol kliensek nem képesek futtatni a használni kívánt alkalmazásokat, de az is lehetséges, hogy más okokból nincs is szükség az alkalmazás kliensen történő futtatására. Ilyen okok lehetnek, az inkompatibilitás, erőforráshiány, illetve az alkalmazás által igényelt központi adatbázis. Érdemes megemlíteni, hogy a terminál szolgáltatás használatánál a programok a szerveren mennek végbe, míg a helyi kliensen csupán egy terminál kliens fut és ezek mellé csak megfelelő sávkapacitás szükséges.

Elsőnek nézzük meg a kliens oldalt. A Windows Vista megjelenésével hozta a változásokat a terminál szolgáltatások terén, ugyanis vele együtt megjelent az Remote Desktop protokoll (RDP) 6-os verziója. Fontos megemlíteni, hogy az RDP telepítésével felkerül az ActiveX is, ami a kliens távoli kapcsolat webes eléréséhez (Remote Desktop Web Access) szükséges. Így olyan gépre is felkerül, ahol az ActiveX vezérlő telepítése tiltva van. Másik újdonság, amit Server 2008-cal jól ki lehet használni, a hálózati szintű hitelesítés (Network Level Authentication - NLA), amely lehetőgét ad arra, hogy hitelesítsünk a kapcsolat kiépítés előtt. Ez védelmi szempontból igazán jelentős fejlesztés. Még egy biztonságot növelő fejlesztés a Transport Layer Security (TLS), ami azért felelős, hogy távoli asztal szolgáltatóhoz kapcsolódás esetén ne egy harmadik fél szerveréhez kapcsolódjunk, aki információkat szerezne meg rólunk. A TLS protokoll a napjainkban népszerű Secure Socket Layer (SSL) protokoll továbbfejlesztése.

A védelmi megoldásokon kívűl természetesen más újítás is van, mégpedig a megjelenítés terén. Növekedett a maximális képernyő felbontás 4096×2048 és a képarányok tárháza és bővült 16:9-es és 16:10-es skálákkal. Ezenkívűl akár saját felbontást beállíthatunk paraméter használatával: mstsc /w: width /h: height vagy az RDP konfigurációs fájljának átírásával. Érdemes még megemlíteni, hogy többmonitoros megjelenítési üzemmód támogatása is bekerült a szolgáltatásokhoz. Ezt a /span kacsoló segítségével aktiválhatjuk, melynek hatására kiterjeszthetjük az asztalt. Azok a felhasználók, akik grafikus programokat használnak nagy újítás lehet, hogy mostmár 32 biten keresztül láthatják a távoli asztalt. Ezen felül még bekerült egy ClearType (Font Smoothing) funkció is, amelyet nagy sávszélesség mellett érdemes használni, mivel akár tízszeresére is megnőhet a sávterhelés.
A nyomtatás terén is bővült egy új funkcióval, mégpedig az EasyPint-tel. Ez a szolgáltatás azt előzi meg, hogy telepítenünk kelljen a kliensnél elhelyezkedő nyomtató kezelő programját a szerverre. Így továbbra is tudunk nyomtatni, mégpedig olyan módon, hogy a szerver egy XPS formátumban küldi el a nyomtatandó dokumentumot a kliensenk. Ezt a kliens operációs rendszere feldolgozza és továbbküldi a nyomtatónak.
Az új kliensek letölthetőek Windows Server 2003-ra és Windows XP SP2-re is, viszont egyes funkciók nem lesznek elérhetőek ezen rendszerek alatt (pl.: NLA).
A fentebb említett bővítéseken kívűl még más új szolgáltatások is megjelentek a Windows Server 2008-ban, melyekről a lentebb olvashatunk.

IV.4.1 TSRemoteApps

Terminálszolgáltatások Távoli Alkalmazásoknak, angol nevén Terminal Service Remote Applications (TS Remote Apps) a felhasználók számára a leghasznosabb és leglátványosabb fejlesztés. A RemoteApp a távoli alkalmazások zökkenőmentes futtatására ad megoldást. Segítségével a távoli alkalmazások úgy fognak futni, mintha azok a saját gépünkre lennének telepítve.
A legtöbb biztonsági adminisztrátor el szeretné érni, hogy minden felhasználóknak csak a legszükségesebb privilégiumai legyenek meg. Ez még inkább igaz a távoli belépő kapcsolódások számára. Álmatlan éjszakákat okozhat azon gondolkozni, hogy hogyan biztosítsunk teljes távoli asztal kapcsolódásokat a nem admin felhasználóknak. Abban az esetben, hogy ha az egyik igazolt felhasználó egy hacker, akkor teljes asztali környezet kerülhet az irányítása alá, így veszélyeztetve a hálózatunkat. Valóban szükséges a felhasználóknak teljes elérés az asztalhoz? Vagy csak annyira van szükségük, hogy elérjék az

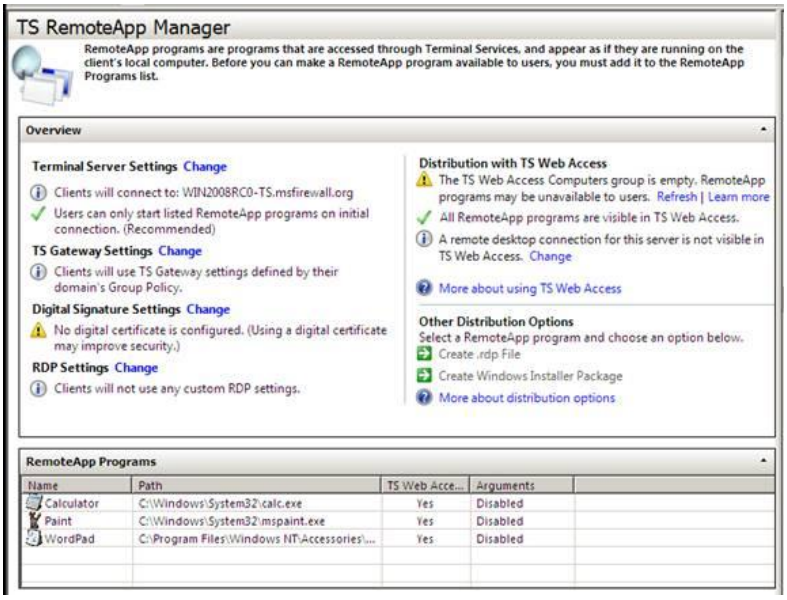
alkalmazásokat az asztalon? Nagyon valószínű hogy csak az alkalmazás és adatok elérésére van szüksége. Nagyon sok vállalatnál még előfordul az is, hogy erőforrás és energia takarossági okokból használják ezt a szolgáltatást, ilyenkor gyakran megesik, hogy csak egy alkalmazást futtatnak.

Erre az esetre megoldást nyújt a Windows Server 2008, melynek a neve Terminál Szolgáltatások Távoli Alkalmazásoknak, angol nevén Terminal Service RemoteApps. Terminál Szolgáltatások Távoli Alkalmazásoknak megengedi, hogy csak a kijelölt alkalmazások számára adjunk elérést az RDP csatornán, azaz RemoteApp képes a programot úgy megjeleníteni, mintha az valóban a klienseken futna. Természetesen valójában nem a kliensen fog futni, de ettől függetlenül elősegíti a kényelmes használatot. Ily módon a felhasználók nem kerülnek bajba a teljes elérésű asztalokkal, és ha egy felhasználónak álcázott hacker próbál belépni, akkor az csak alkalmazásokat fog tudni használni. Így kisebb támadási felületet biztosítunk ellentétben azzal, mintha egy teljes asztalunk lenne.

Több távoli alkalmazás együttes használata esetén a kliensszámítógép mindössze egyetlen terminál kapcsolatot épít fel a kiszolgálóval, a feladatkezelőben jól megkülönböztethetőek a távolról futó programok.

A programokat RDP konfigurációs fájlok formájában is terjeszthetjük, de készíthetünk Windows Installer csomagokat is, melyeket aztán csoportházirend segítségével juttathatunk a kliensekre, hivatkozást hagyva a Start menüben vagy akár az asztalon, így felhasználóink úgy használhatják ezeket a távoli programokat, mintha ténylegesen a saját munkaállomásaikon kerültek volna telepítésre.

A Terminál Szolgáltatások Távoli Alkalmazásoknak nagyon rugalmas. Irányítani tudjuk melyik alkalmazást érheti el a felhasználó és hogyan érhetik el az alkalmazásokat a saját számítógépükön. TS Távoli Alkalmazásoknak a TS Átjáróval együtt a Windows Server 2008 Terminál Szervert értékessé teszik minden olyan vállalat számára, akik érdekeltek a biztonságos RDP alapú távoli elérésekben. Az 17. ábrán látható a TS Távoli Alkalmazásoknak menedzser konzolja. Felállítani egy TS Távoli Alkalmazásoknak nagyon könnyű és elég hamar futásra is tudjuk bírni.



17. ábra A TS RemoteApp kezelőfelülete

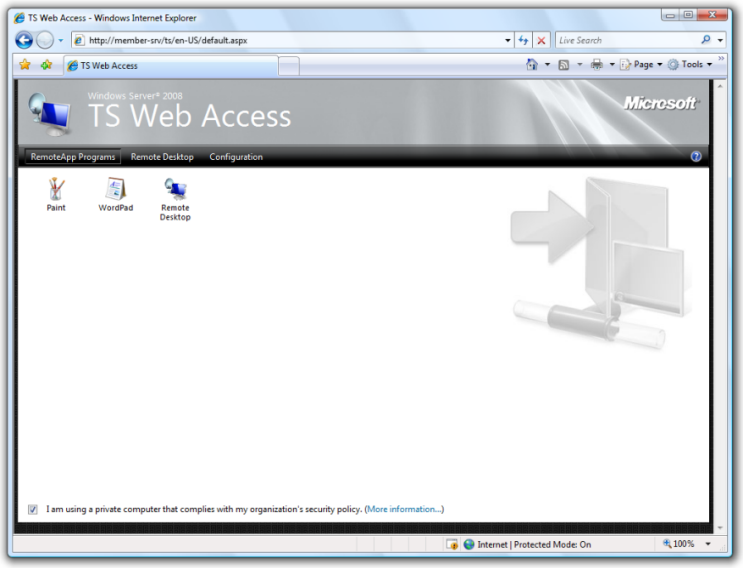
A 17. ábra mutatja, hogy mit lát a felhasználó az asztalán mikor elindítja a RemoteApps -t. A Properties szöveg dobozban láthatjuk, hogy az elérési út egy .rdp kiterjesztésű fájlra van beállítva, amely megengedi hogy meghatározott elérés legyen az egyes alkalmazásokhoz.

IV.4.2 TS Web Access

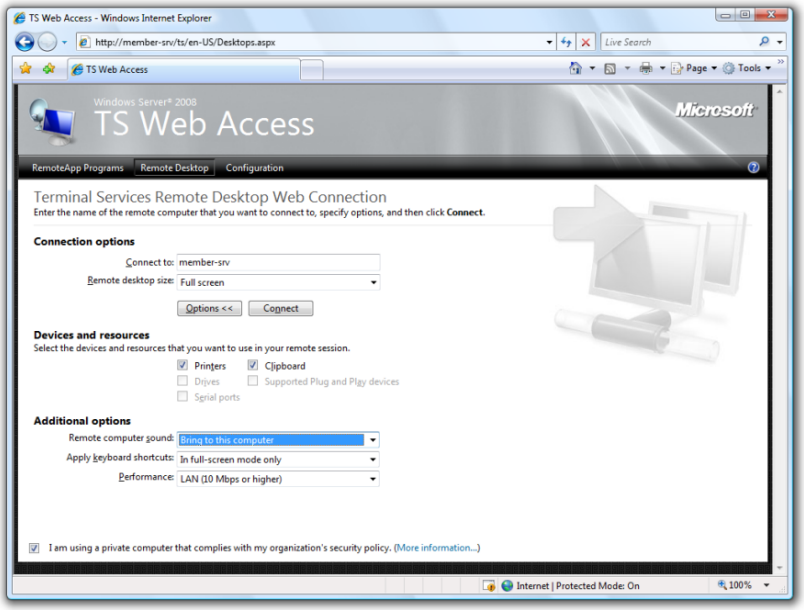
Ahogy már az korábbi fejezetben is szó esett róla, a Windows Server 2008-nak van TS Web Acces szolgáltatása is. Az ezt megelőző verziókban a felhasználó először egy ActiveX vezérlőt használva a böngészőjén keresztül csatlakozhatott a s terminál kiszolgálóhoz, így elérhette a weben keresztül a távoli asztalt. A probléma akkor következett be, hogy ha a felhasználónak nem volt jogosultsága az ActiveX telepítésére, így nem volt lehetősége ilyen módszerrel elérni a távoli gépet. Mindez az RDP kliens 6-os verziójával megoldódott

A fejlesztések során a Web Acces szolgáltatás ötvözve lett az előző fejezetben tárgyalt RemoteApp szolgáltatással, ezzel lehetőségünk van arra, hogy publikált alkalmazásokat indítsunk el webes felületen keresztül.

A Web Acces kezelőfelülete jelentős változásokon ment át, a béta verziók alatt is többször átalakult. Itt látható minden olyan alkalmazás, melyek elérhetőek számunkra a webes kliensen keresztül, valamint ha adtunk jogosultságot a terminál csatlakozás számára, az szintén megjelenik itt. Ezzel egy lehetőséget kapunk az olyan programok elindítására, melyeket nem telepítettünk a kliensekre a korábbiakban említett módon. Természetesen ebben az esetben is a saját "asztalunkon" indulnak el a programok, nem pedig a böngészőben.



18. ábra TS Web Acces kezelőfelülete



19. ábra Ts Web Acces csatlakozási felülete

Akár azt is megtehetjük, hogy integráljuk a TS Web Part –ot az általunk készített weblapon vagy belső Sharepoint oldalon is. A Web Part a Web Access oldalnak az a része, amerre az elérhető programok listáját láthatjuk.

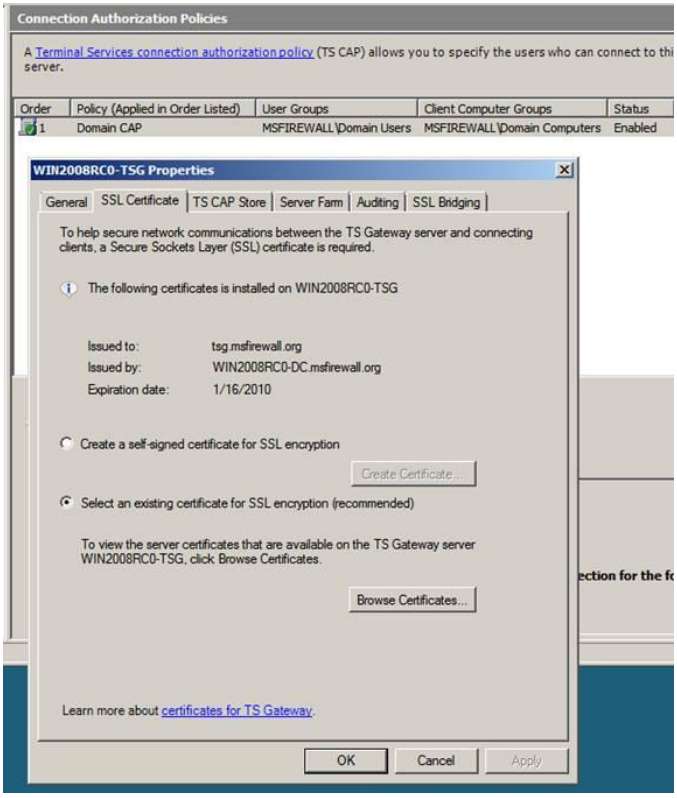
IV.4.3 Terminál Szolgáltatások Átjáró

Terminál Szolgáltatások Átjáró, angol nevén Terminal Services Gateway (TS Gateway) főképp olyan helyeken fog nagy sikeret aratni, ahol eddig virtuális magánhálózatot, más néven Virtual Private Network-t (VPN) használtak a terminál szerver elérése végett.

A teljes terminálszolgáltatás kiépítésének egyik akadálya a megbízhatatlan hitelesítési módszer és az RDP csatornák titkosítási szintje volt, a másik pedig az, hogy sok tűzfal a távoli helyen nem engedte a kimenő forgalmat TCP 3389 porton.
Hasonlót a VPN használatával is elérhettünk, de olyankor probléma léphetett fel ha publikus helyről akartuk elérni a vállalati hálózatott, ugyanis vagy a vállalati tűzfal vagy a helyi hálózat tűzfala blokkolta a kapcsolódáshoz szükséges protokollokat, portokat.
A TS Gateway használatával tehát nem csak egyszerűbb, de biztonságosabb is lesz a terminálszolgáltatások elérése külső hálózatból. Így csak egyetlen port, a 443-as megnyitására van szükség, amely általában engedélyezve van a vállalati környezetekben, már csak a HTTPS kapcsolattal történő böngészés miatt is.
A Terminál Szolgáltatások Átjáró egyfajta SSL a VPN-n, ugyanolyan módon mint a RPC/HTTP az Outlook számára, hogy elérje az Exchange Server-t. Az SSL VPN valójában egy alkalmazás protokoll proxi. A TS Átjáró együttműködik az RDP 6.0+ kliensekkel, hogy megengedettek legyenek a beágyazott RDP kapcsolódások a TS Átjáró számítógéphez. Az RDP kliens valójában beágyazza az RDP protokollt két másik protokolba. Elsőnek, az RDP protokoll be van ágyazva az RPC fejrészbe, valamint még egyszer a kódolt HTTP fejrészrészébe. A protokoll, amit a TS Átjáró kapcsolódásához használunk valójában egy RDP/RPC/HTTP protokoll. Microsoft valószinűleg azért tette ezt, hogy használni tudják a meglévő RPC/HTTP kódot, ami már megvolt az RPC/HTTP proxijuk számára.
Mikor a kapcsolódunk a TS Átjáró géphez, a TS Átjáró eltávolítja az RPC és HTTP fejrészt és továbbküldi az RDP kapcsolatot a megfelelő Terminál Szerver vagy Távoli Asztali számítógéphez, azaz a kliens a 443-as porton keresztül éri el az átjárót, innen pedig a szokásos TCP 3389-es porton keresztül történik a kapcsolódás a terminál szerverhez. Van lehetőség arra, hogy telepítsük a két szolgáltatást ugyanazon számítógépre, de ez nem ajánlott. Pontosan be tudjuk állítani, hogy mely felhasználók, mely számítógépekről, milyen erőforrásokhoz férhetnek hozzá a hálózatunkban. Az ilyen beállításokra a RAP (Resource Authorization Policy) és a CAP (Connection Authorization Policy) házirendek állnak rendelkezésre, azonban növelhetjük a biztonságot ha az ISA Server + TS Gateway + NAP Server modellt alkalmazzuk. Ily módon a hálózati adatforgalom az ISA kiszolgálóig HTTPS, a belső hálózaton pedig már normál HTTP protokollon keresztül zajlik, mivel az ISA képes eltávolítani a kapcsolat tanúsítványát. Ilyenkor már a forgalmat szűrni tudjuk a tűzfal szabályaival is, valamint a NAP Server megvizsgálhatja a számítógépek egészségét és a szabályozás szerint engedélyezheti vagy tilthatja a hálózati elérést. Megfelelő állapot esetén

következik a TS Gateway és az előbb említett módon engedélyezi a hozzáférést a meghatározott erőforrásokhoz.

Az 20. ábrán láthatjuk az interfészt a Kapcsolat Hitelesítési Házirend (KHH) létrehozás számára. A KHH-t használjuk, hogy eldöntsük melyik felhasználó érheti el az erőforrásokat ezen a TS Átjáró számítógépen keresztül. A beszéd panel az ábrán megmutatja a beállítás interfészt az azonosítás megkötések számára a TS Átjáró oldalon, így csak a biztonságos SSL kapcsolódások engedélyezettek.



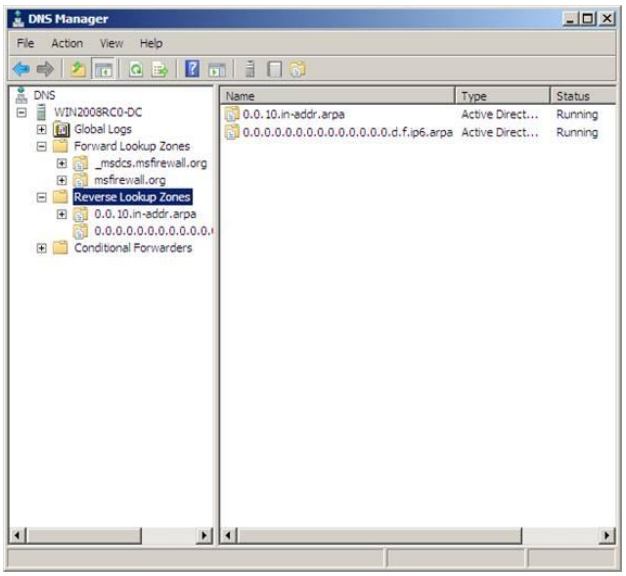
20. ábra SSL kódolás beállítása

Terminál Szolgáltatások Átjáró az Okos Kártya hitelesítést is támogatja és megvan az a lehetőségünk, hogy ráerőltessük a NAP kliens belépés vezérlést.

IV.5 Natív IPv6 támogatás

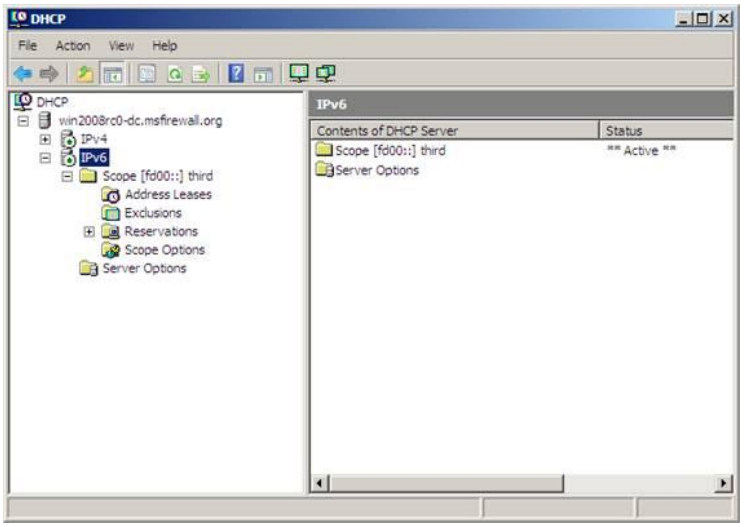
A Windows Server 2008 az első olyan verziójú Windows Server amelynek van IPv6 támogatása mint egyetlen IP halmaz része. Az előző verziókban a Vista előtti korszakban, az IPv6 támogatás párhuzamos volt az IPv4-gyel, és nem volt beépített támogatás az IPv6 számára beleszámítva a hálózat infrastruktúra szolgáltatásokat is mint DNS és DHCP. Mostantól nem ez a helyzet és az IPv6 szorosan bele lett szőve a Windows Server 2008 hálózati halmaz és infrastruka szolgáltatásokba. A 21. ábrán látható, hogy a Windows Server

2008 DNS-e most már támogatja az IPv6-t. Létre tudunk hozni négyes A (AAAA) rekordokat és még IPv6 fordítva kereső zónákat is.



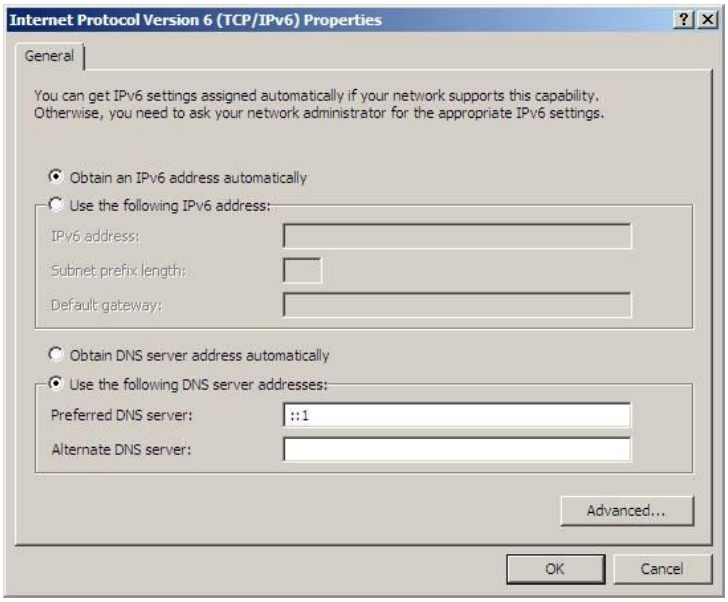
21. ábra A DNS IPv6 támogatással

A DHCP szolgáltatás szintúgy fel lett frissítve, hogy támogassa az IPv6-t. Az 22. ábrán láthatjuk, hogy létrehoztunk egy DHCP hatáskört az egyedi helyi címek számára.



22. ábra DHCP IPv6 támogatása

A 23. ábra mutatja, hogy be tudjuk állítani a hálózati interfészt, hogy statikus IPv6-t címezzen vagy DHCP-t használjanak IP címezési információkra.



23. ábra IPv6 tulajdonságok

Windows Server 2008 RRAS szervereket (amelyek routerként viselkednek), mostantól be tudjuk állítani IPv6-os routernek, valamint információkat tudnak adni (az forgalomirányítási üzenetekkel) attól függően, hogy a kliens milyen prefix információt használ, ezenkívűl használjanak-e alapos címzési információt a DHCP szerverktől is.

Windows Server 2008 még az átmeneti IPv6 technológiákat is támogatja, úgymint az ISATAP-t, 6to4-t és Teredo-t. Bármelyik Windows Server 2008 számítógépet be lehet állítani egy ISATAP routernek a Netsh parancssor interfész használatával.

IV.6 Read Only Domain Controllers

A szervezetek kirendeltségeinek elterjedésével, sokan felismerték a hitelesítés problémáját. A kirendeltségeket gyakran ellátják egy tartomány vezérlővel, mely felhasználói helyi tartományvezérlőnél tudnak hitelesítést kérni. Így nem kell, hogy átmenjenek egy lassú vagy talán megszakadt WAN kapcsolaton, ami hitelesítés hibákat okozhat és még a helyi erőforrások hozzáférését is akadályozza.

A megoldás az volt, hogy tegyük a tartomány vezérlőket a kirendeltségekbe. Amíg ez megoldotta a kezdeti hitelesítési problémát addig felvetett egy másik biztonsági jellegűt. Mivel a legtöbb kirendeltségnek nincs ugyanolyan szintű IT szakképzettsége, és fizika biztonsága, mint a főirodában, így a kirendeltség tartomány vezérlője vált a leggyengébb láncszemmé az egész Active Directory infrastruktúrában. Az olyan változtatások, amelyeket a nem szakértő felhasználók hajtottak végre a kirendeltségnél, az az egész szervezetre hatással

lehetett. Ha a tartomány vezérlőt ellopták a kirendeltségből, akkor az potenciálisan veszélyes volt az összes vállalati felhasználó számára.

A Windows Szerver 2008 megoldása a csak olvasható tartományvezérlő, angol nevén Read Only Domain Controller . Ez tartalmazza egy csak olvasható másolatát az Active Directory adatbázisnak és csak a kirendeltség felhasználói fiókjait tárolja. Mivel nem lehet megváltoztatni az Active Directoryt rajta, így nem kell félnünk, hogy egy képzetlen felhasználó visszavonhatatlan változtatásokat tesz. Valamint mivel tipikusan nincs adminisztrátor szintű felhasználó a kirendeltségeknél, így relatíve kicsi a kockázat olyan esetben, hogy ha ellopják a tartomány vezérlőt kirendeltségből, mivel nem tárol magas jogosúltságú fiókot.

A csak olvasható tartomány vezérlőt be lehet állítani, hogy bizonyos felhasználói fiókokat csak átmenetileg tároljon. Így a tartományvezérlő ellopásának bekövetkezése esetén az átmenetileg tárolt felhasználói információk listája elérhető a főirodában dolgozó Active Directory adminisztrátor számára. Ezzel lehetséges, hogy az Active Directory admin letiltsa vagy újrabeállítsa a jelszavakat ezeken a felhasználói fiókok számára a főirodában.

IV.6.1 Administrative Role Separation

Delegálni tudjuk a helyi adminisztárotori engedélyeket a RODC szervernél bármely felhasználó számára. A delegált felhasználói fiókoknak mostantól lehetőségük lesz belépni a szerverre és megcsinálhatják a szerver karbantartási feladatokat. Mindezt anélkül, hogy lenne bármilyen AD DS (aktív könyvtár tartmány szolgáltatás) engedélyük és ezenkívűl a felhasználónak nincs engedélye más tartomány vezérlőkhöz az Aktív könyvtárban. Így a biztonság nincs kiszolgáltatva a tartományban.

IV.6.2 Read-Only DNS

Pluszban a RODC-hez lehetőség van feltelepíteni egy DNS szolgáltatást. Egy DNS szerver ami RODC-n fut nem támogatja a dinamikus frissítéseket, de a klienseknek lehetősége van arra, hogy használják névfeloldás lekérdezésére.

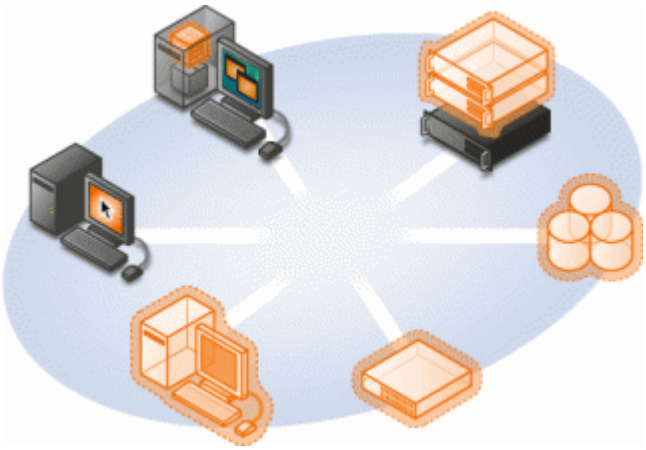
Mivel a DNS csak olvasható, a kliensek nem tudják frissíteni a rekordokat rajta, de ha egy kliens frissíteni akarja a saját DNS rekordjait, a RODC el fog küldeni egy beszámolót egy írható DNS-nek. Az egyszerű frissített rekord ezekután ki lesz cserélve az olvasható DNS-en az írható DNS-től kapott információk alapján. Ez egy speciális egyszerű objektum (DNS

rekord) csere, hogy a RODC DNS szerver friss maradjon és a kirendeltségeknél gyorsabb névfeloldást hajtson végre.

IV.7 Hyper-V

A virtualizációs piacon jelenleg két szereplő van, aki méreténél fogva jelentős: a VMware és a Microsoft. A Microsoft az új termékével minden olyan ember igényét kielégíti, aki ingyen vágyott a VMware termékére.

A Hyper-V a Windows Server 2008 hipervisora, ami megengedi nekünk, hogy virtuális gépet futtasunk a számítógépünkön. Elődje a Virtual Server 2005, és mivel a Hyper-V-t integrálták a rendszerbe, így nem jár plusz költséggel. Ezenkívűl megjelent egy Windows Server 2008-tól független változat is, a Hyper-V Server 2008, melynek jelenleg R2-es változata van piacon. A Hyper-V Server 2008 ingyenesen letölthető a Microsoft honlapjáról.



A Hyper-V egy szerepkör a Windows Server 2008-ban és olyan eszközöket és szolgáltatásokat nyújt, melyek segítségével létrehozni és menedzselni tudunk virtualizált szerver számítógép környezetet. Ez a virtuálizált környezet azért hasznos, mert kezelhetünk virtuális gépeket benne, valamint ezen környezet segítségével lehetségessé válik több számítógép futtatása, (akár különböző fajtájú operációs rendszerrel) ugyanazon fizikai számítógépen. Ugyanakkor e virtuális környezetben vagy azt választjuk, hogy elzárjuk egymástól a virtuális gépeket, vagy specifikálhatjuk hogyan kommunikálhatnak egymás között, valamint egy külső hálózattal.

Sok fizikai szervert (kb. 40-50) üzemeltető vállalalatoknál eljön az az idő, mikor a hardverkörnyezet sokszínűvé válik úgy korban, mint technológiai fejlettségben és állapotban, hogy a fenntartásuk és karbantartásuk egyre több erőforrást emészt fel. Egyre nagyobb hely, áramellátás iránti igény, valamint hűtési problémák lépnek fel ilyenkor. A kábelrengetegből könnyen Gordiuszi csomó válhat, a rackszekrények megtelnek és egy forró nyári időszakban sorra állhatnak le a ventilátorok, utánna a szerverek is.

Ha ilyen helyzetbe kerülünk, hamar arra jutunk, hogy a hardver környezet cseréje nem vezet megoldáshoz. Bár van arra lehetőség, hogy nagy szerversűrűséget nyújtó megoldásokat

vásároljunk, amik akár középvállalatoknak is megfizethetőek - ilyenek például IBM és HP Magyarországon is nagy számban működő blade rendszerei – de így a problémát csak részben oldjuk meg, ugyanis bizonyos szoftverek csak a régi hardvereken hajldóak futni, és manapság még ezeket megközelítőt sem találunk a piacon.

Az új típusú szerverek „túl jók" a régebbi, kisebb fenntartási költséggel járó szerver-alkalmazások számára. Önálló hardveren futtatva őket, azt észlelhetjük, hogy a ma népszerű két- vagy többmagos processzorokat nem terhelik meg, a kihasználtságuk jócskán 50% alatt marad.

Így oda jutunk, hogy szükségessé válik a szoftveres környezet sűrűségének bővítése, azaz a szervervirtualizáció kiépítése.

Virtuális szerverek használata esetén, a hardveren futó (parent) operációs rendszer olyan elkülönülő virtuális gépeket hoz létre, melyeknek paramétereit pontosan meghatározhatjuk. Beállíthatjuk a prioritást, azaz azt, hogy virtuális szerverek közül melyik kapja előnyösebben az erőforrást a másikkal szemben, valamint mennyi memóriát és processzort használhat, és a hálózati csatlakozókat hogyan használhatja.

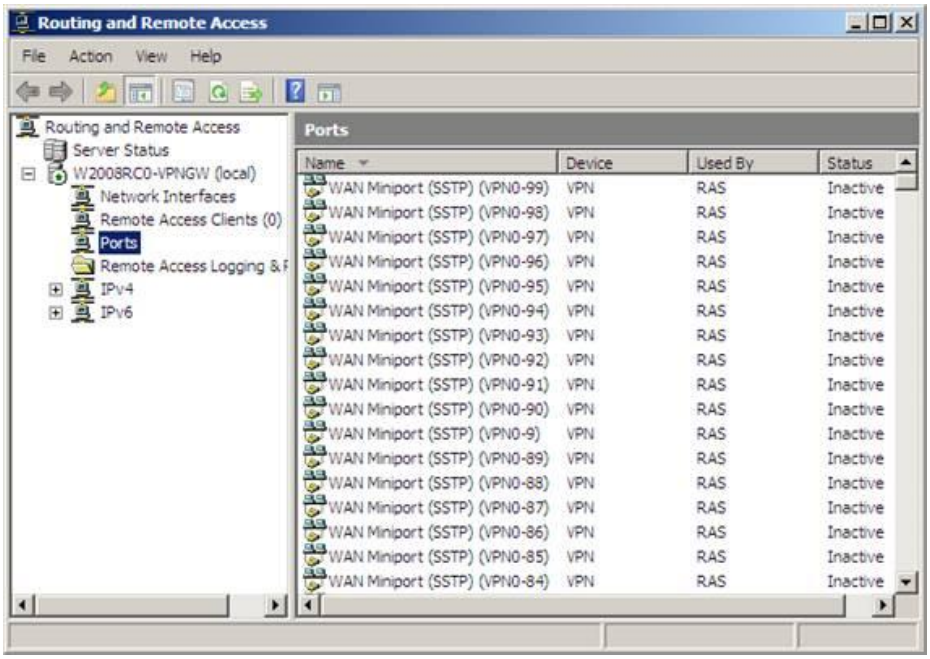
Még egy újdonság, hogy mindegyik operációs rendszer saját driver-set-ét használhatja, így nem muszáj közös meghajtókon osztozniuk. Ezzel az új technológiával gyorsabb, illetve hatékonyabb lett a működés. A virtuális szerverek mostantól nem virtuális HUB-on, hanem switch-en keresztül kapcsolódhatnak egymáshoz. Valamint bekerült a VLAN és a NAP támogatás is. A VSS snapshot módszerei ugyancsak elérhetőek lesznek számunkra, így az erre alapozó mentési metódusok szintén használhatóak. A virtuális környezet kezelésére is kapunk megoldást, méghozzá a System Center család tagjaként elérhető Virtual Machine Manager nevezetű szoftvert. A szülő operációs rendszerek kezelésére továbbiakban is az Operations és a Configuration Manager programok állnak rendelkezésünkre. A feladatátvevő fürtök által növelhetjük a rendszerek rendelkezésre állási idejét, még abban az esetben is, ha különböző fizikai paraméterrel rendelkező szervereket használunk. A különböző fizikai csomópontokon futó és csomópontonként akár több különböző virtuális szervert futtató fürt esetén is megvalósítható, hogy nem tervezett leállás esetén a virtuális szerverek áthelyezésre kerüljenek a megfelelően működő szerverekre. Itt lehet megjegyezni, hogy a Microsoft virtualizációs technológiája akár 16 csomópontos fürtön is képés működni.

Szoftverfejlesztéssel foglalkozó cégeknek szintén jól jöhet a Hyper-V, mivel használatával egy egységes futtatókörnyezetet tudnak kialakítani. Ezt az előre leírható virtuális környezetet sablonként is lehet használni.

IV.8 Secure Socket Tunneling Protocol (SSTP)

A Biztonságos Socket Csatornázási Protokoll, angolul The Secure Socket Tunneling Protocol (SSTP) egy igazi SSL virtuális magánhálózat. Amit igazi alatt értünk az az, hogy az SSL VPN egy SSTP amely teljes hálózati szinten nyújt VPN hozzáférést a vállalati hálózaton, ugyanolyan módon mint a PPTP és a L2TP/IPSec. Azonban az SSTP előnye a PPTP-vel és L2TP/IPSec-kel szemben, hogy, nem kell aggódnunk amiatt, hogy tűzfalak megakadályozzák a kimenő kapcsolódásokat az SSTP-hez.

Az SSTP lényegében PPP/SSL, mivel a PPP kapcsolatok bele vannak ágyazva egy biztonságos HTTP fejrészbe (SSL), SSTP át tud menni bármilyen tűzfalon vagy Web proxi eszközön ami engedélyezi a kimenő SSL-t. Többé nem lesz olyan hívás a felhasználóktól a hotelekből vagy konferencia centrumokból akik panaszkodnak mert a tűzfal az ottani helyükről nem engedi be őket a VPN hálózatra. Egy másik jó dolog az SSTP esetén az, hogy nem kell engedélyezni a kimenő kapcsolódásokat az SSTP-hez mivel elég csak az SSL kimenő forgalmát engedélyezni. Van egy érték a CONNECT fejrészben amit be tudunk állítani az ISA tűzfalon vagy más alkalmazás réteg figyelő tűzfalon ami megengedi nekünk, hogy letiltsuk a SSTP kapcsolódásokat míg az egyéb SSL kapcsolatokat engedélyezzük. Az SSTP sokkal könnyebbé fogja tenni az életünket távolról kapcsolódó VPN kapcsolatok esetén.

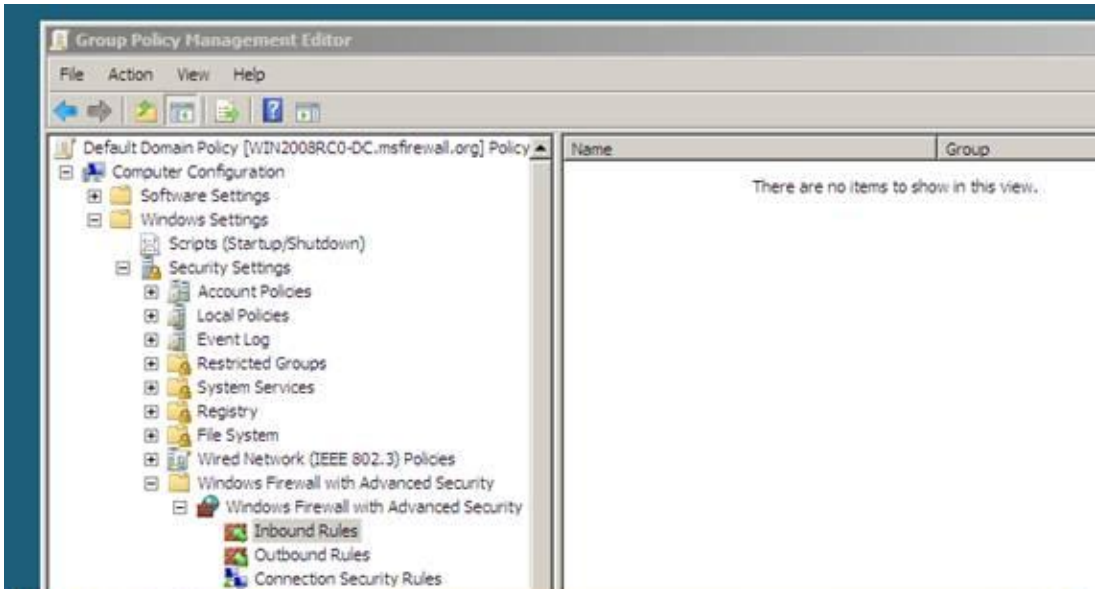


24. ábra Távoli kapcsolat port beállításai

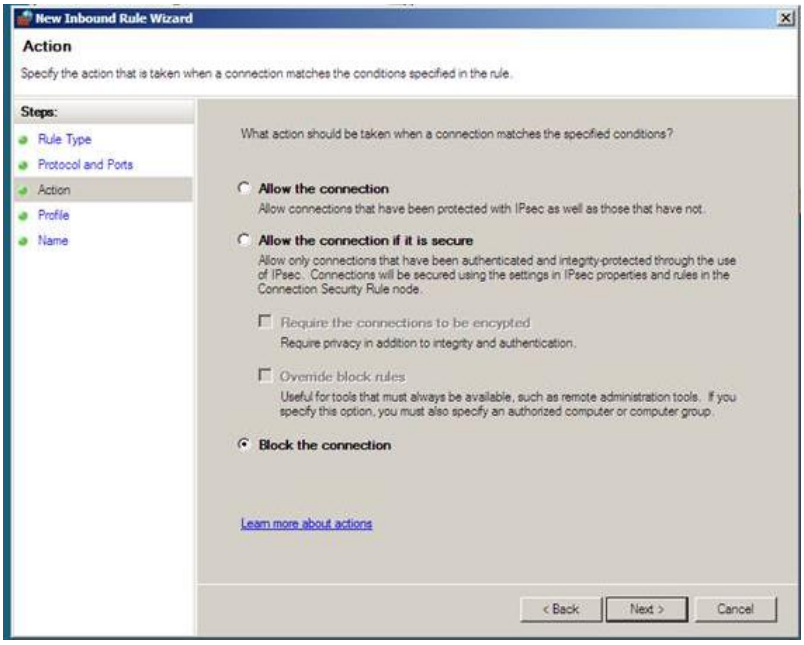
IV.9 Windows Advanced Firewall és Policy Based QoS

A Windows Vista felhasználók felismerik a Haladó Windows Tűzfalat, angol nevén Windows Advanced Firewall-t. A Windows Server 2008-cal ugyanazokat az előnyöket kapjuk, mint a Vista felhasználók. Ami még jobb is az az, hogy használhatjuk a csoport házirendet a Windows Server 2008-ban átfogó centralizást menedzsmentjeként a Haladó Windows Tűzfalnak. Ennek segítségével finom hangolást csinálhatunk a bejövő és kimenő forgalomra. A kimenő forgalom vezérlés volt a hiányzó darabkája a Windows XP tűzfalának. Mostantól irányíthatjuk a kimenő forgalmat, így ha észrevesszük, hogy vannak férgekkel fertőzött állomások és ezek egy bizonyos vagy csoportos portot céloznak, akkor le tudjuk tiltani ezokat a portokat mindegyik állomáson a csoportos házirenden keresztül.

Az 25. ábrán látható az „Új beérkező forgalom szabályok” varázsló. A varázsló, amit használhatunk a csoportos házirend menedzsment konzolban, lehetővé teszi, hogy nagyon könnyen beállítsuk a bejövő forgalom szabályokat. Emellett van még „Kimenő forgalom szabály” varázsló, amely segítségével le tudjuk tiltani a kimenő forgalmat, UDP és TCP portokon, ICMP üzenet tipusokon egyaránt, vagy tiltani tudunk alkalmazáson alapokon is.

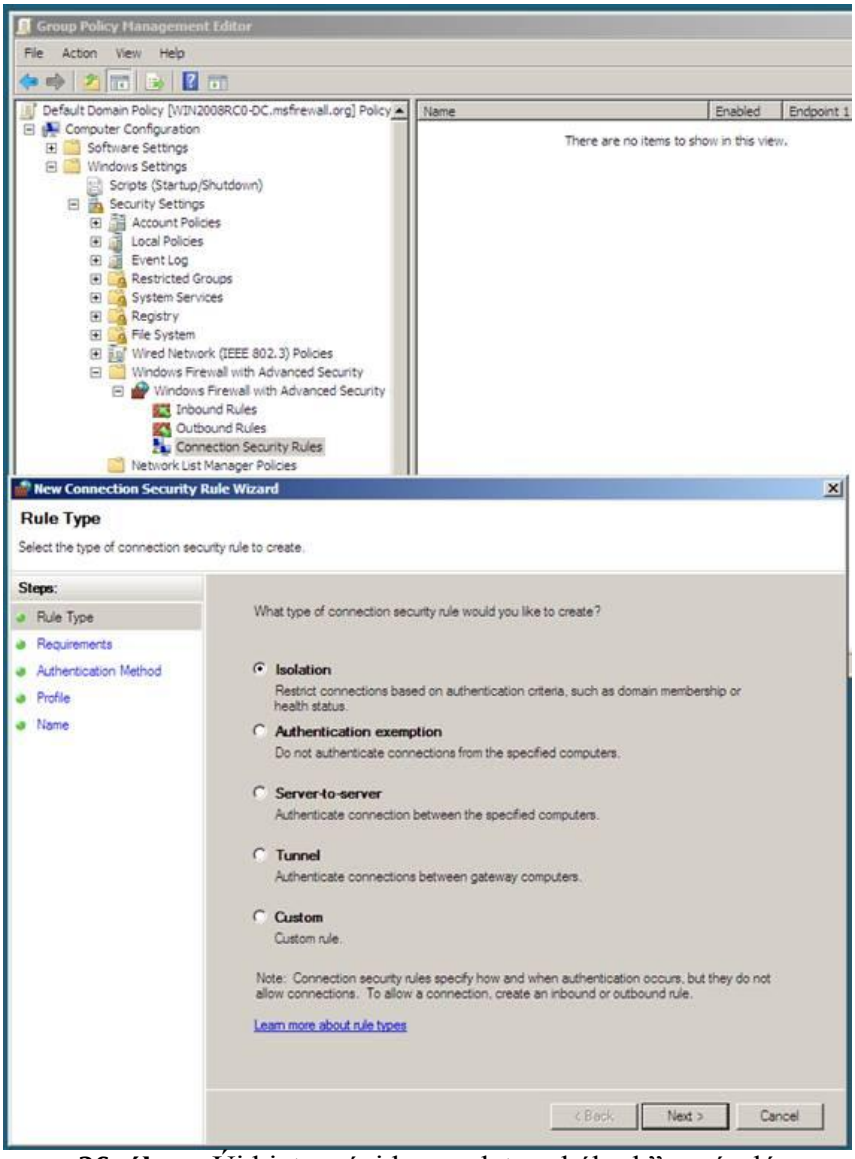


25/1. ábra beérkező forgalom szabályai



25/2. ábra az „Új beérkező forgalom szabályok” varázsló

Az egyik nagyszerű tulajdonsága a Windows tűzfalnak, hogy milyen egyszerűvé lett téve a IPSec házirendend létrehozása. A múltban az IPSec házirend beállítása egy kicsit ’vagy sikerül vagy nem’ alapon ment. Végig kellett mennünk a varázslón és reménykedhettünk, hogy mindent rendesen beállít. Mostantól nem ez a helyzet Haladó Windows Tűzfallal. Az 26. ábra mutatja, hogy milyen könnyű használni az „Új biztonsági kapcsolatok szabály” varázslót, ami egyszerűvé teszi az IPSec tartomány elhatárolás házirendek létrehozását, hitelesítés mentesség házirendeket, a szolgáltatónak egy másik szolgáltatóhoz IPSec kapcsolódásokat és IPSec csatornákat.

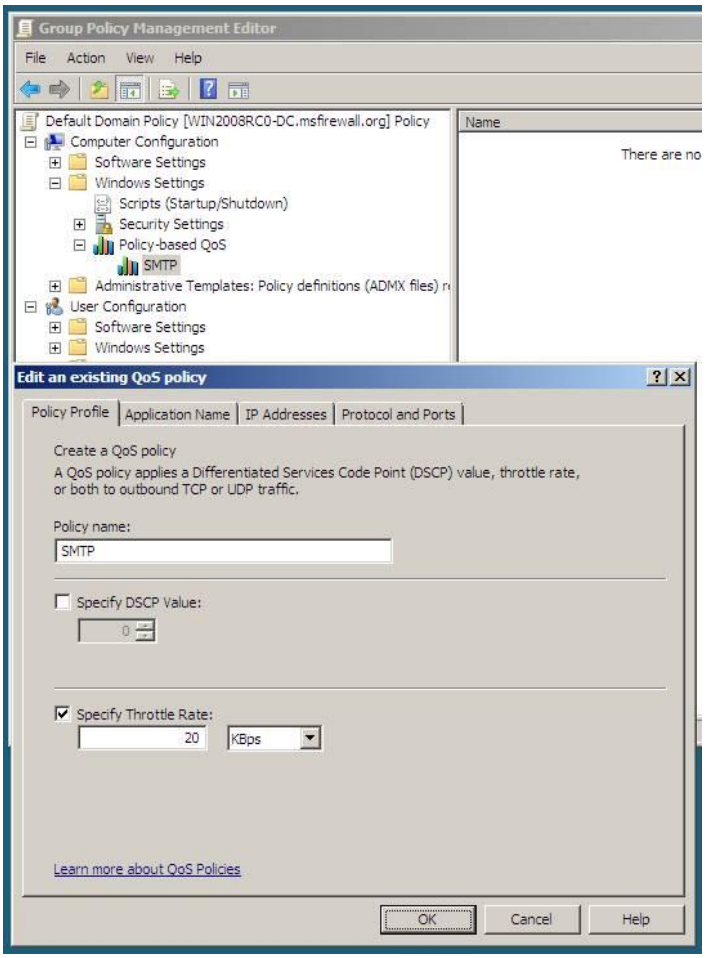


26. ábra „Új biztonsági kapcsolat szabályok” varázsló

Egy másik nagy fejlesztés a Windows Server 2008-ban, hogy centralizálódott a QoS házirend menedzsment a csoportos házirenden keresztül. Előző verziókban volt QoS tulajdonság, de mivel nem igazán volt standardizálva, így nem sok ember (ha egyáltalán valaki) használta. Mostantól ez másképp lesz az új házirend alapú QoS tulajdonsággal, amit rögtön használhatunk is.

Két módja van, hogy implementáljuk a QoS házirendeket, kemény kódolással átállíthatjuk az értékeket vagy előnyt kovácsolhatunk a Differentiated Services Code Point (DSCP) értékekből, amik a hálózati routereken vannak beállítva. Azonban még ha nincs is DSCP engedélyezett routerünk vagy még nem használtuk a DSCP-t még mindig van arra lehetőség, hogy beállítsuk a házirendeket, így a helyi állomások rákényszerítődnek az átviteli vezérlőre a TCP vagy UDP portokon egyaránt, valamint specifikált alkalmazásokon.

A 27. ábra egy QoS házirendet mutat, ami az SMTP protokollt irányítja a végállomás porton, az a TCP 25-ön. Ki tudjuk választani melyik állomásra legyen igaz ez a házirend. Például, ha nem akarjuk, hogy az SMTP szerverünk le legyen korlátozva, de a többi állomást a hálózatunkon le akarjuk korlátozni a SMTP forgalmában. Ily módon, irányítani tudjuk mennyi spam fertőzött számítógép küldjön e-mailt, mielőtt észrevennénk a fertőzést.



27. ábra

V. Hálózati megoldások

Ebben a fejezetben ismeretetni fogok a lehetőségek közül néhányat, amik megmutatják, hogy a Windows Server 2008 milyen professzionális módszereket alkalmaz a hálózati infrastruktúrában.

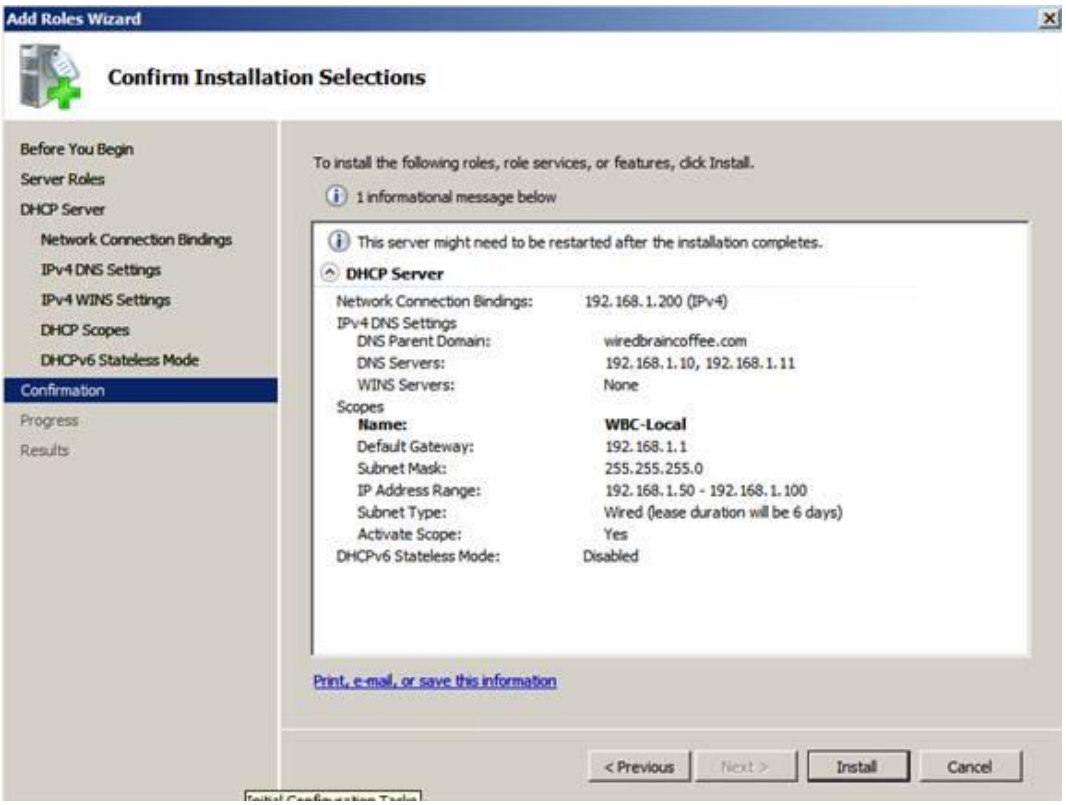
V.1 DHCP

A dinamikus állomáskonfiguráló protokoll angol nevén Dynamic Host Configuration Protocol, segítségével oldható meg, hogy a végpontok automatikusan megkapják a hálózat használatához szükséges információkat. Ilyen például az IP cím, hálózati mask, alapértelmezett átjáró, stb.

V.1.1 Telepítés

A Windows Server 2008 DHCP szerver telepítése ezentúl sokkal egyszerűbb lesz, mivel egy szerepkörré vált, és nem egy komponens többé, mint az ahogy korábbi verziókban volt.
Ahhoz hogy ezt létrehozzuk, kell egy feltelepített és bekonfigurált Windows Server 2008 rendszer statikus IP címmel. Ismernünk kell a hálózat IP készletét, azaz azt hogy mik a kiosztható címek, mik a DNS szerver IP címei, valamint az alapértelmezett átjárót is. Ezenkívűl meg kell tervezni minden kapcsolódó alhálózatot, hogy milyen szerepkörük legyen és hogy milyen kizárásokat akarunk létrehozni.
Ahhoz, hogy elkezdjük a DHCP telepítési folyamatát, rá kell kattintani az Add Roles-ra az Initial Configuration Task ablakban, vagy kiválasztjun a Server Manager menüpontban a, Roles és végül Add Roles almenüpontot.
Mikor az Add Roles Wizard ablak felugrik rákattinthatunk a Next gombra az ablakon. Következőnek válasszuk ki a DHCP Server Role-t és kattintsunk a Next-re. Ha nincs beállítva a statikus IP a szerver számára, akkor egy kapunk egy figyelmeztetést, hogy ne telepítsük a DHCP-t dinamikus ip címmel. Ezen a ponton elkezdjük az IP hálózat, szerepkörök és a DNS beállításait. Ha úgy akarjuk feltelepíteni a DHCP szervert, hogy ne legyenek az előbbiek beállítva, akkor egyszerűen a Next-re kattintva kihagyjuk ezt a procedúrát. Másrészről viszont érdemes beállítani a DHCP szerver ezen részét. Esetünkben mi kapunk a lehetőségen és beállítunk pár alap IP beállítást és DHCP szerepkört. Ezekután a varázsló megmutatja a „network connection binding”-t, magyarul a halózat csatlakozási megkötéseket és megkér minket a megerősítésére. Amit valójában a varázsló kérdezne az az volna, hogy milyen

interfészen keresztül akarunk DHCP szolgáltatásokat nyújtani. Mi az alapot választjuk ki, aztán a Next –re kattintunk. Következőként beírjuk a Parent Domain -t, Primary DNS Server, és Alternate DNS Server-t és a Next-re kattintunk. Most azt választjuk, hogy ne használja a WINS-t a hálózatunkon és utána a Next-re kattintunk. Ezekután felugrik egy ablak, amely segítségével beállíthatjuk a DHCP hatáskörét az új DHCP szerverünknek. Állítsuk be az 192.168.1.50-100 készletet, hogy lefedjünk 25+ PC klienst a helyi hálózatunkban. Ehhez kattintsunk az Add-ra, hogy hozzáadjunk új hatáskört. Mint ahogy az 28. ábrán is látható lesz, elneveztük a hatáskört WBC-Local –nak, be lett állítva a kezdő és vég IP címek 192.168.50-192.168.1.100-ig, az alhálózati maszk 255.255.255.0, az alapértelmezett átjáró 192.168.1.1, az alhálózat típusa kábeles és végül a hatáskör aktiválása is. Menjünk vissza az Add Scope ablakra, kattintsunk a Next-re , hogy hozzáadjuk az új hatáskört(miután a DHCP szerverünk feltelepült). Válasszuk ki a DHCPv6 stateless mode tiltását ezen szerver számára és kattintsunk a Next-re. Végül erősítsük meg a DHCP telepítési beállításainkat és kattintsunk az Install-ra.

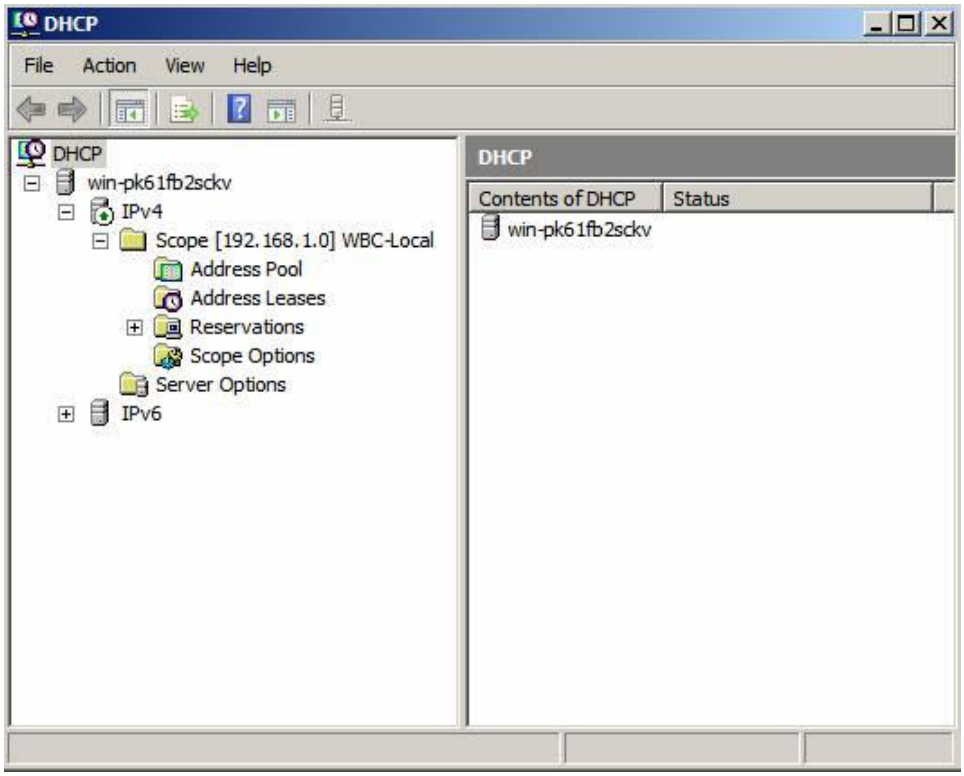


28. ábra DHCP beállításainak megerősítése

Rendes esetben egy pár másodperc után feltelepül a DHCP szerverünk és erről egy ablak is tájékoztat minket. Ezt be is zárhatjuk a Close gombbal, majd folytathatjuk a munkát a DHCP szerverünk menedzselésével.

V.1.2 Menedzselés

A telepítéshez hasonlóan, a Windows Server 2008 DHCP szerver menedzselése is könnyűnek mondható. A Szerver Menedzserben, a szerepeknél kattintsunk az új DHCP szerver bejegyzésre. Míg a DHCP szerver hatáskörét és a klienseket nem tudjuk vezérelni innen, addig azt viszont tudjuk vezérelni az eseményeket, szolgáltatásokat és forrásokat, amik a DHCP szerverünkhöz kapcsolódnak. Így ez egy megfelelő hely arra, hogy megnézzük az állapotát, és hogy milyen események történtek körülötte. Azonban, hogy valóban konfigurálni tudjuk a DHCP Szervert és lássuk, hogy milyen kliensek kaptak IP címeket, használnunk kell a DHCP szerver MMC-t. Ehhez a Start menüben, az Administrative Tools almenüt kell választanunk és a DHCP Server –re kell kattintanunk. Mikor ez megnyílik, egy halom lehetőséggel találjuk szembe magunkat, mint ahogy az 29. ábrán is látható.



29. ábra A Windows Szerver 2008 DHCP MMC

A DHCP Server MMC mindenféle információt ad nekünk, ilyenek pl.: IPv4, IPv6, hatáskörök, cím készlet, elengedések, foglalások, hatásköri opciók stb. Ha a címkészletre és szerepkör opciókra megyünk, láthatjuk, hogy milyen beállításokat tettünk meg mikor feltelepítettük DHCP szerverünket. Láthatjuk a címtartományt az alapértelmezett átjáró címét, és azt, hogy beállításaink sikerültek-e. Ahhoz, hoy valójában megbizonyosodjunk róla, hogy megfelelően működik tesztelnünk kell. Ezt meg is tesszük a következő részben.

V.1.3 Működés teszt

Ahhoz, hogy teszteljük szükségünk lesz egy kliensre. Jelen esetben mi egy Windows Vista kliens fogunk használni, ami ugyanabban a hálózati szegmensben található, mint a szerverünk. Ahhoz, hogy biztosak legyünk benne, ne használjunk egyelőre másik eszközt ebben a hálózatban. Parancssorban írjuk be: IPCONFIG /RELEASE, majd IPCONFIG /RENEW. Ha minden rendben van, akkor a DHCP szervertől kapunk egy IP címet. Menjünk vissza a szerverünkhöz és itt is megerősíthetjük, hogy valóban van egy új Vista kliens a listában. Ezzel megbizonyosodtunk a működésről és végeztünk is.

V.2 Active Directory Domain Services

Korai változatai 1999-ben jelentek meg, majd később a végleges verzió a Windows 2000 szerverben látott napvilágot. A Windows Server 2003 bővítette szolgáltatáskészletekkel és javította adminisztrációs lehetőségeit. További előrelépések történtek a Windows Server 2003 R2 és a Windows Server 2008-as változatokban, ahol az Active Directory Domain Services nevet kapta.

Az Aktív Könyvtár Tartomány Szolgáltatások, vagy angol nevén Active Directory Domain Services (régebben csak Active Directory) szolgáltatásoknak egy összefoglaló neve, melyek a következők:

- Active Directory Domain Services (AD DS)
- Active Directory Federation Services (AD FS)
- Active Directory Lightweight Directory Services (AD LDS)
- Active Directory Rights Management Services (AD RMS).
- Active Directory Certificate Services (AD CS)

Mindegyik szolgáltatás egy szerepkört reprezentál, ez egy új megközelítés a Windows Server 2008-ban.

V.2.1 Az újdonságok

Sok újdonság jelent meg, melyekből a követekezőket emelném ki:

- Csak Olvasható Tartomány Vezérlő (Erről már esett szó a korábbiakban)
- Újraindítható Aktív Könyvtár Tartomány Szolgáltatások
- Finomszemcsézettségű jelszó házirendek

V.2.2 Restartable Active Directory Domain Services

Mostantól meg tudjuk állítani és újratudjuk indítani az AD DS-t, ami annyit jelent, hogy el tudunk végezni bizonyos feladatokat és karbantartást anélkül, hogy újraindítanánk a szervert. Korábbi verziókra jellemző volt, hogy szükséges volt szerver újraindítása és ezekután Könyvtári Szolgáltatások Helyreállítási módban kellett indítani a szervert. Ezentúl e nagyszerű megoldás segítségével szkriptelhetőek és automatizálhatóak lesznek ezek a feladatok. Az AD DS lehetséges állapotai: elindítva, leállítva, helyreállítási üzemmód. Hasznos olyan feladatoknál amelyeknél szükséges volt az újraindítás, hogy az AD DS ki legyen kapcsolva. Ez flexibilitást ad az adminisztátoroknak, akik így az AD DS karbantártásokat gyorsabban el tudják végezni.

V.2.3 Finomszemcsézettségű jelszó házirendek

Csak egy jelszavunk és fiókunk lehet tartományonkét a kizárás házirendnek megfelelően, ami minden felhasználóra vonatkozik a tartományban. Újdonságként a finomszemcsézettségű házirendekkel különböző fajta jelszavakat vagy kizárás házirendeket határozhatunk meg a különböző felhasználói csoportok számára azonos tartományon belül. A következő beállításokra lesz lehetőség:

Jelszó házirendek:

- Enforce password history
- Maximum password age
- Minimum password age
- Minimum password length
- Passwords must meet complexity requirements
- Store passwords using reversible encryption

Kizárás házirendek:

- Account lockout duration
- Account lockout threshold
- Reset account lockout after

A finomszemcsézettségű házirendeket felhasználói objektumokra és globális biztonsági csoportokra tudjuk vonatkoztatni. Az nem lehetséges, hogy OU-sokra vonatkoztassuk.

V.2.4 Federation Services Föderációs Szolgáltatások

A Windows Server 2003 R2-ben jelent meg először és azonosító elérés megoldásokat nyújt. Böngésző alapú klienseket ad, amik kívűl vagy belül vannak a hálózatunkon, Single-Sign-On (SSO). Fontos megjegyezni, hogy az FS csak web alapú alkalmazásokkal működik és web hoszt vagy SharePoint környezetben lehet használni. Nagyon hasznos mikor egy vállalatnak a webszerverei a DMZ-ben (Data Management Zone), vagy távoli hosztnál, vagy üzletpartnernél vannak és a vállalat irányítani akarja a fiók igazolást a web alkalamzásaiohoz a belső Aktív Könyvtárból.

V.2.5 Az AK FS újdonságai

Viszonylag új technológia a Microsoft-tól, és ez a termék második generációja. Új funkciók jelennek meg amik könnyítik a felső adminisztrációt és kibővítik a kulcs Microsoft alkalmazások támogatását. Egy áttekintés az új funciókról:
Haladó telepítés: Az AK FS szerver szerepkörként került be a Windows Server 2008-ba és validációs vizsgálatokat is tettek bele a telepítés varázslóba. A Szervermenedzser automatikusan kilistázza és telepíti az összes szolgáltatás amely szükséges az AK FS számára annak szerepköri telepítése során.
Haladó alkalmazás támogatás: Az új verzió még szorosabban be lett integrálva az Aktív Könyvtár Jogok Menedzselési Szolgáltatásokba és a Microsoft Office Sharpoint Szerverbe (MOSS). A MOSS 2007 mostantól kezdve támogatja a Single-Sign-On (SSO) képességeket, amik integrálva vannak az AK FS-ben. Az AK FS ezentúl támogatja a MOSS 2007 tagság és szerepkör szolgáltatókat, ami azt jelenti, hogy be tudjuk állítani a MOSS 2007-et mint óvatos alkalmazást az AK FS-ben, és akkor adminisztrál bármilyen SharePoint oldalt, tagság és szerepkör alapú belépés vezélést használva.
Jobb adminisztrációs tapasztalat, mikor föderációs bizalommal dolgozunk: Az AD FS egy bizalom házirend importálással lett bővítve, valamint funkcionalitás exportálással, hogy segítse minimalizálni a partner alapú konfigurációs problémákat.

V.2.6 Az Ak FS működése

Az AK FS segítségével a nagy vállalatok szelektíven lehetnek nyitottak az infrastruktúrájukban a megbízható partnereik és vásárlóik felé. Három mag képességet nyújt:

- Extranet authentication

- Web single-sign-on
- Identity federation services for IIS-based Web applications

AK FS arra lett tervezve, hogy telepítve legyen olyan közép és nagy vállalatokban, amelyek rendelkeznek a következők valamelyikével:

- Legalább egy könyvtár szolgáltatás: vagy aktív könyvtár tortomány szolgáltatás (AD DS) vagy aktív könyvtár könnyűsúlyú könyvtár szolgáltatás (AD LDS)
- Tartománykapcsolt számítógépek
- Különböző operációs rendszer platformot futtató számítógépek
- Számítógépek melyek internethez kapcsolódnak
- Egy vagy több Web alapú alkalmazás

Minden kommunikáció az AK- től kezdve az AK FS-ig le van kódolva és mindegyik kommunikáció a kliensektől az AK FS –ig SSL –lel van kódolva.

A föderációs környezet hasznossága abban rejlik, hogy mindegyik vállalat folytathatja a saját azonosítói menedzselését, de emellett védeni tudják a projekteket, és el tudnak fogadni másik vállalattól azonosítókat.

V.2.7 Szerepkörök az AK FS-ben

Különböző szerepkörök vannak attól függően, hogy milyen vállalati igény lép fel. Telepíthetünk szervereket egy vagy több AK FS szerepkörrel is, íme egy áttekintés róluk:

- **Föderációs szolgáltatások:** használhatja egy vagy több föderációs szerver, hogy megosszon közös bizalom házirendet. A föderációs szerverek arra vannak kitalálva, hogy irányítsák a hitelesítés kérést a felhasználói fiókoktól, melyek más vállalatnál vannak vagy interneten keresztül csatlakoznak
- **Föderációs szolgáltatások proxy:** egy olyan proxy, mely a Föderációs Szolgáltatások számára lett kitalálva a kerületi hálózatban (DMZ). WS-Föderációs Passzív Kérő Profilt portokolt használ (angol nevén WS-Federation Passive Requestor Profile, WS-F PRP), hogy összegyűjtse a felhasználói tanusítványokat a böngészős kliensekből és elküldje ezeket a Föderációs Szolgáltatások számára.
- **Igény figyelő ügynök:** a Web szerverre van telepítve, mely hosztolja az igény figyelő alkalmazásokat. Szükséges engedélyezni az AK FS biztonsági token igény lekérdezését. Egy igény-figyelő alkalmazás vagy egy Microsoft ASP.NET alkalmazás vagy egy alap alkalmazás, mint a MOSS 2007.

- **Windows token alapú ügynök:** fel lehet telepíteni a Web szerverre ami hosztolja Windows NT token alapú alkalmazásait. Szükséges, hogy támogassa az átalakításokat egy AK FS biztonsági token-ról egy tolmács-szintig. A Windows NT token alapú módszer egy olyan alkalmazás, mely a Windows alapú hitelesítési mechanizmust használja.

V.2.8 AK FS és a Server Core

Nem része a Szerver Core-nak, ez amiatt van, hogy függőségben van az ASP.NET-tel, ami nem elérhető a Szerver Core alatt.

V.2.9 Telepítés

Az AK FS egy olyan tulajdonság, ami segít a fejlesztőknek akik Web-alapú alkalmazásokat készítenek. Ez lehet a kulcs, hogy biztonságos külső elérést nyújtson a Web alkalmazások számára. Együtt használható az Atív könyvtár Könnyűsúlyú Könyvtár Szolgáltatásokkal (AK KKS), mint egy azonosító nyújtó a hitelesítés számára, hogy elérjék a házirend alapú irányítást, azaz egy teljes megoldást nyújt arra, hogy kibővítsük a Web alapú alkalmazásokat egy megbízható szövetkezet számára.

V.2.10Könnyűsúlyú Könyvtár Szolgáltatások

Korábban Aktív Könyvtár Alkalmazás Mód, angolul Active Directory Application Mode (ADAM) néven volt ismeretes. Egy speciális mód az AK számára, melyben a könyvtári szolgáltatások kizárólagosan az alkalmazások számára vannak beállítva. Ezzel nyújt mind tárolást és elérhetőséget az alkalmazások számára, ugyanazt az interfészt használva, amit már az adminisztrátorok és fejlesztők már értenek.

Az AK KKS egy LDAP könyvtár szolgáltatás adat tárolás és visszaállítás könyvtár engedélyezett alkalmazások számára, a függőségek nélkül szükséges az AK KS számára. Emellett nem tárol biztonsági szempontokat, amiket az AK KS tárol. A fejlesztők használhatják az AK KKS-t, hogy dolgozzanak az Aktív Könytár információkkal az alkalmazásaikban. Az AK FS egy az alkalmazások közül, amelyek azért használják az AK LKK-t, hogy hitelesítési információkat tároljanak.

VI. Összefoglalás

Dolgozatomban ismertettem a Windows Server 2008 számtalan fontos szolgáltatásai közül azokat, amelyek a legtöbb hálózatban megjelennek, valamint az újdonságait. Dolgozatom célja a hálózatüzemeltetés főbb momentumainak, a kiadás újdágainak valamint a Windows Server 2008 által támasztott lehetőségek bemutatása volt. Remélem, hogy a felvonultatott szolgáltatások és technikák hasznosak voltak az Olvasó számára.

VII. Irodalomjegyzék

http://www.microsoft.com/windowsserver2008/
http://www.microsoft.com/en/us/default.aspx
http://technet.microsoft.com/
http://www.windowsnetworking.com/
http://winportal.net/
http://www.w3schools.com/browsers/browsers_os.asp
http://wikipedia.org/
http://lepenyet.spaces.live.com/
http://www.rufusz.hu/
http://www.microsoft.com/video/en/us/details/806bb329-55a0-4be2-89d2-bb5e8d7dd808

VIII. Köszönetnyilvánítás

Köszönettel tartozom témavezetőmnek, Dr. Krausz Tamásnak a szakmai irányításért és a dolgozatom megírásához szükséges források biztosításáért, továbbá a felmerülő szakmai kérdésekre adott válaszaiért.